Benutzerhandbuch

IKOM-Router LAN

Copyright © CAT Dorfer Consulting GmbH

Die in dieser Publikation veröffentlichen Beiträge sind urheberrechtlich geschützt. Übersetzungen, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen bedürfen der ausdrücklichen Genehmigung der CAT Dorfer Consulting GmbH.
Alle Rechte vorbehalten.

CAT Dorfer Consulting GmbH
Kampstrasse 7a
D-24616 Hardebek
Tel: +49 4324-88634
Fax: +49 4324-88635
Internet: http://www.cat-t.de
email: info@ccat-t.de

Technische Änderungen vorbehalten.
Alle Warenzeichen und Produktbezeichnungen sind Warenzeichen, eingetragene Warenzeichen oder Produktbezeichnungen der jeweiligen Inhaber.
Alle Lieferungen und Leistungen erbringt die CAT Dorfer Consulting GmbH auf der Grundlage der Allgemeinen Geschäftsbedingungen der CAT Dorfer Consulting GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da..

Produkt-Nr.: 266-00

Inhalt

Technische Daten **5**
Hardware Installation **6**
Anschlussbelegung 6
LED Anzeigen 7
Konfiguration WBM **8**
Start der Konfiguration 8
Device Information **9**
Hardware 9
Software 10
Status **11**
Network Connections 11
I/O Status 12
Routing Table 12
DHCP Leases 13
Local Network **14**
IP Configuration 14
DHCP Server 15
Static Routes 16
Wide Area Network **17**
WAN Setup 17
Static Address 18
DHCP Client 19
PPPoE 20
Static Routes 21
DynDNS 22
Connection Check 23
Network Security **24**
General Setup 24
Firewall 25
NAT Table 26
VPN **27**
IPsec 28
Connections 28
Connections Settings 29
Connection IKE 31
Certificates 33
Status 34

Inhalt

OpenVPN 35
Tunnel 35
Port Forwarding 37
Certificates 38
Static Keys 39
Status 40
I/O 41
Inputs 41
Alarmierung per SMS 42
Einrichten eines Email zu SMS Gateway 42
Outputs 43
Socket Server 44
System 45
Web Configuration 45
User 46
Log Configuration 47
Log-File 48
SMTP Configuration 49
Configuration Up-/Download 50
Konfiguration über SSH und XML-Datei 51
Download der Konfiguration per SSH 51
Upload der Konfiguration per SSH 51
RTC 52
Reboot 53
Firmware Update 54
Abfrage und Steuerung über XML Dateien 55
Format der XML Dateien 55
Beispiele zu den Basis-Einträgen: 55
a) E/A System 55
Daten senden und empfangen 57
Funktions-Test 58
Applikationsbeispiel 59

Technische Daten

Versorgung

Versorgungsspannung	10 V DC ... 30 V DC über steckbare Schraubklemme
Nennstromaufnahme	< 90 mA bei 24 V
LED-Anzeige	Power (LED grün) Dauerlicht: Betrieb

Schnittstellen

Router	
Protokolle/ Dienste	DHCP-Server, HTTP-Server, FTP, NAT, Firewall, SMS, OpenVPN, IPSec, DynDNS, NTP
VPN	Sichere Datenverschlüsselung mit IPSec und Open VPN (inkl. X.509 Unterstützung
Ethernet-Schnittstelle	
Anschlussart	2xRJ45-Buchse, geschirmt
Übertragungsrate	10/100 MBit/s
Unterstützte Protokolle	TCP/IP, UDP/IP, FTP, HTTP
Hilfsprotokolle	ARP, DHCP, PING(ICMP), SNMP V1, SMTP
LED-Anzeige / Steuer-signalindikator	ACT (LED gelb), Ethernet-Datenübertragung LINK (LED grün), Ethernet-Link hergestellt
Serielle Schnittstelle	optional
I/O`s	4 Eingänge, 4 Ausgänge

Physikalische Merkmale

Größe (HxBxT)	101x116 x35 mm
Umgebungstemperatur	Betrieb -25...+60°C, Lagerung -40 …+85°C
Luftfeuchtigkeit	0...95% (nicht kondensierend)
Schutzart	IP20

CE-Konformität gemäß R&TTE-Richtlinie 1999/5/EG

EMV	EN 61000-6-2, EN55022 Class B
Sicherheit	EN 60950
Funk	EN 301511

Zulassungen

cUL, USA / Kanada	in Bearbeitung

Technische Änderungen vorbehalten

Hardware Installation

Anschlussbelegung

Ethernet 1

Ethernet 2

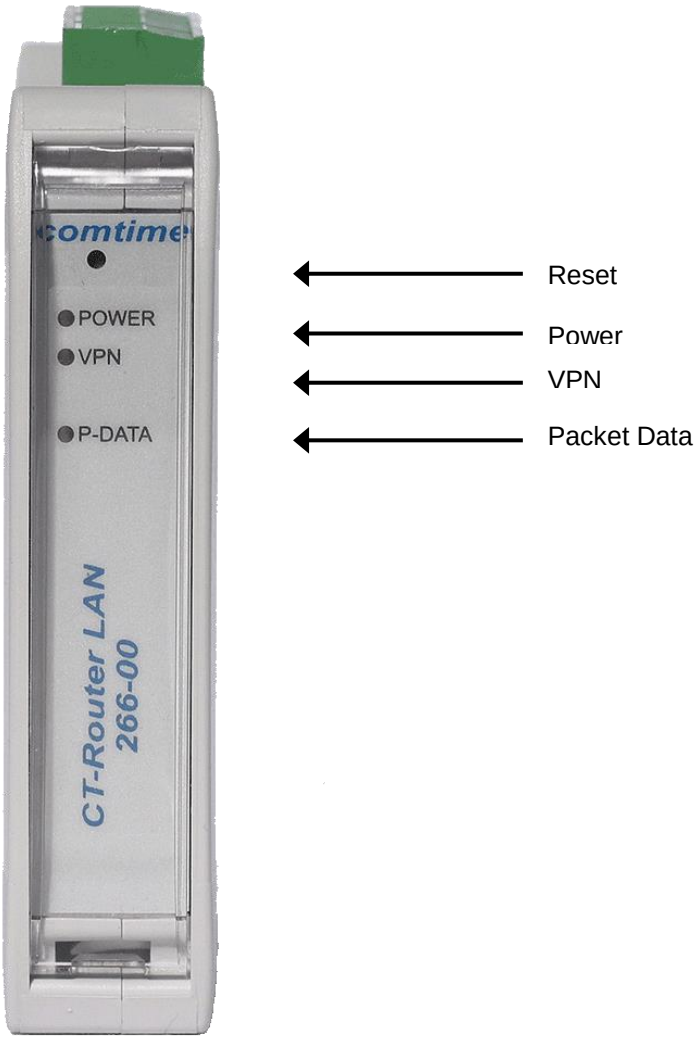
USB

Stromversorgung
10V - 30V DC
0V
NC
NC

Digitaler Ausgang
O4
O3
O2
O1

Digitaler Eingang
I4
I3
I2
I1

LED Anzeigen



LED	Erklärung
Packet Data	Aus = keine Verbindung Blinken = Modem Verbindung Ein = Paketdaten-Verbindung
VPN	Aus = keine VPN-Verbindung Ein = VPN-Verbindung aktiv
Power	Aus = keine Stromversorgung Ein = Stromversorgung aktiv

Konfiguration WBM

Die Konfiguration des Router LAN erfolgt über eine Webbrowser basierende Funktion. Hierfür müssen zunächst folgende Bedingungen erfüllt sein:

- Der Computer, der zur Konfiguration des Routers verwendet wird, verfügt über eine LAN-Schnittstelle.
- Auf dem Computer ist ein Webbrowser installiert (z.B. Google Chrome, Mozilla Firefox, Microsoft Internet Explorer).
- Der Router ist mit einer Spannungsquelle verbunden.

Start der Konfiguration

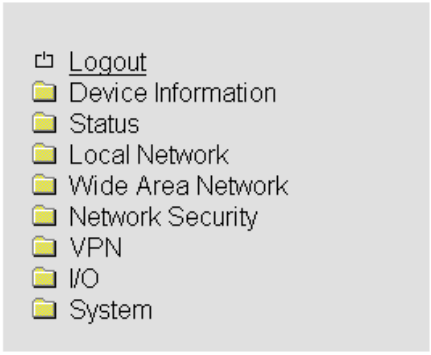
1. Ethernet-Verbindung zwischen Computer und Router herstellen.
2. IP-Adresse der LAN-Schnittstelle auf das Netz des Routers abstimmen.
3. Webbrowser öffnen.
4. Die IP-Adresse des Routers (192.168.0.1) in das Adressfeld des Browsers eingeben und mit Eingabe bestätigen. Anschließend wird eine Benutzername/Passwort-Abfrage erfolgen.

Authentifizierung erforderlich
Für den Server http://192.168.0.1:80 ist ein Nutzername und ein Passwort erforderlich. Der Server meldet Folgendes: Web Server Authentication.
Nutzername:
Passwort:
Anmelden
Abbrechen

Im Auslieferungszustand lautet der Benutzername „admin“ und das Passwort „admin“ (das Ändern des Passwortes wird im späteren Verlauf beschrieben).
Des Weiteren gibt es zwei User-Level:

- User: Lesezugriff auf „Device Information“
- Admin: Lese- und Schreibzugriff auf alle Bereiche

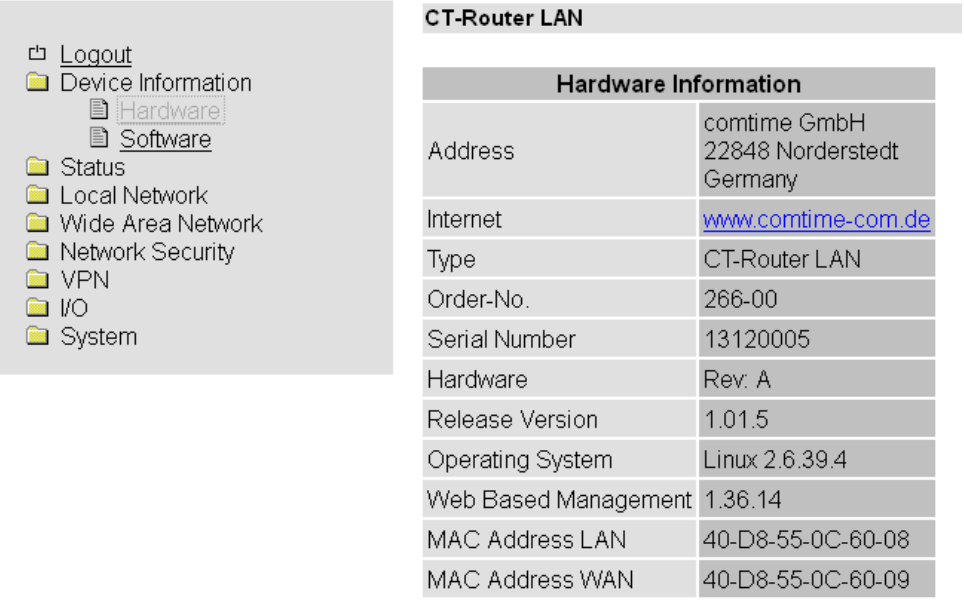
Nach der Eingabe des Benutzernamens und des Passwortes öffnet sich das Hauptmenü zur Konfiguration des Router LAN.



Device Information

In diesem Bereich können Sie genauere Informationen zur eingebauten Hardware, sowie der installierten Software einsehen.

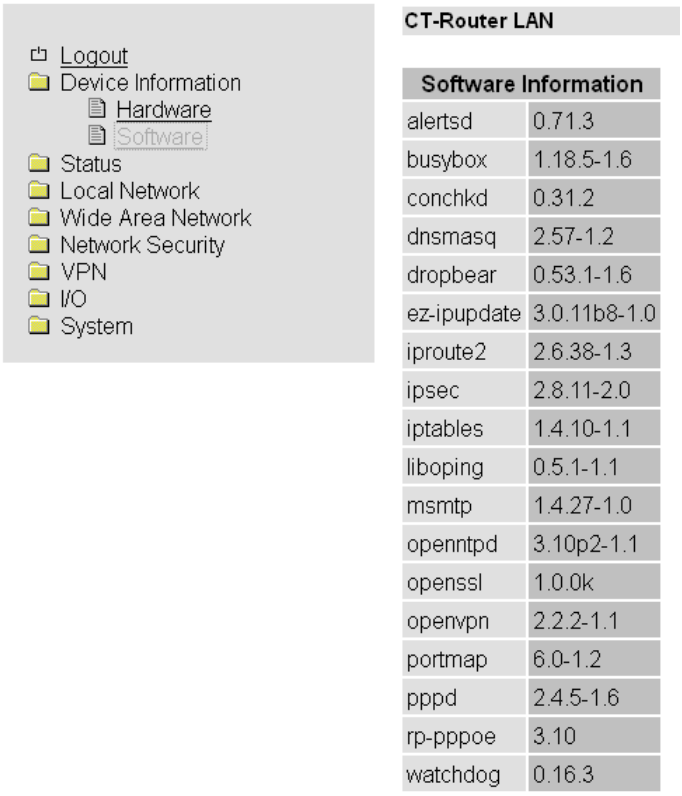
Hardware



Tabellarische Übersicht der eingebauten Hardware.

Device Information

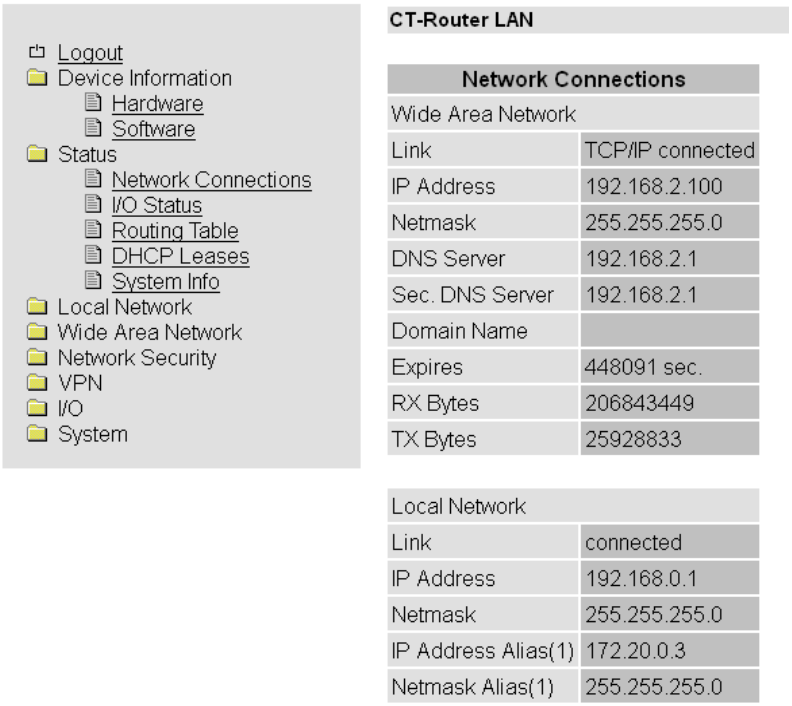
Software



Software Information	
alertsd	0.71.3
busybox	1.18.5-1.6
conchkd	0.31.2
dnsmasq	2.57-1.2
dropbear	0.53.1-1.6
ez-ipupdate	3.0.11b8-1.0
iproute2	2.6.38-1.3
ipsec	2.8.11-2.0
iptables	1.4.10-1.1
liboping	0.5.1-1.1
msmtp	1.4.27-1.0
openntpd	3.10p2-1.1
openssl	1.0.0k
openvpn	2.2.2-1.1
portmap	6.0-1.2
pppd	2.4.5-1.6
rp-pppoe	3.10
watchdog	0.16.3

Tabellarische Übersicht der auf dem CT-Router HSPA installierten Software.

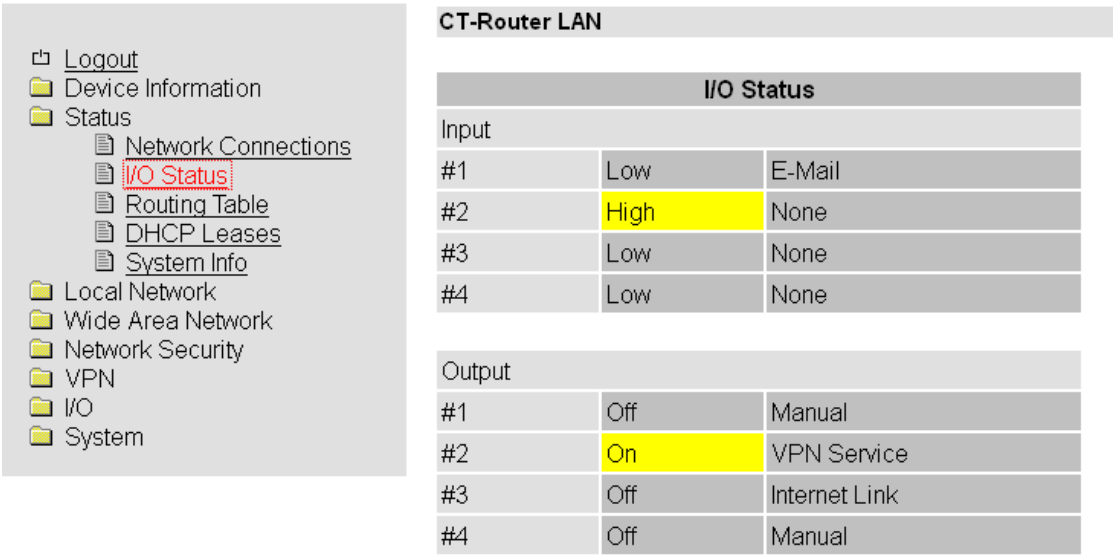
Network Connections



Status → Network Connections	
Network Conncetions	Erklärung
Wide Area Network	
Link	**TCP/IP connected:** TCP/IP Verbindung aufgebaut. **VPN connected:** VPN Verbindung aufgebaut. **not connected:** Es besteht keine aktive Verbindung
IP Address	zugewiesene IP-Adresse (Providervorgabe)
Netmask	zugewiesene Netzmaske (Providervorgabe)
DNS Server	DNS-Server IP-Adresse
Sec. DNS Server	alternative DNS-Server IP-Adresse
RX Bytes	Anzahl der empfangenen Daten seit dem letzten Login in Bytes.
TX Bytes	Anzahl der gesendeten Daten seit dem letzten Login in Bytes.
Local Network	
Link	**connected:** Lokale Ethernet-Verbindung aufgebaut **not connected:** keine lokale Ethernet-Verbindung aufgebaut
IP Address	Ethernet IP-Adresse
Netmask	Ethernet Netzmaske

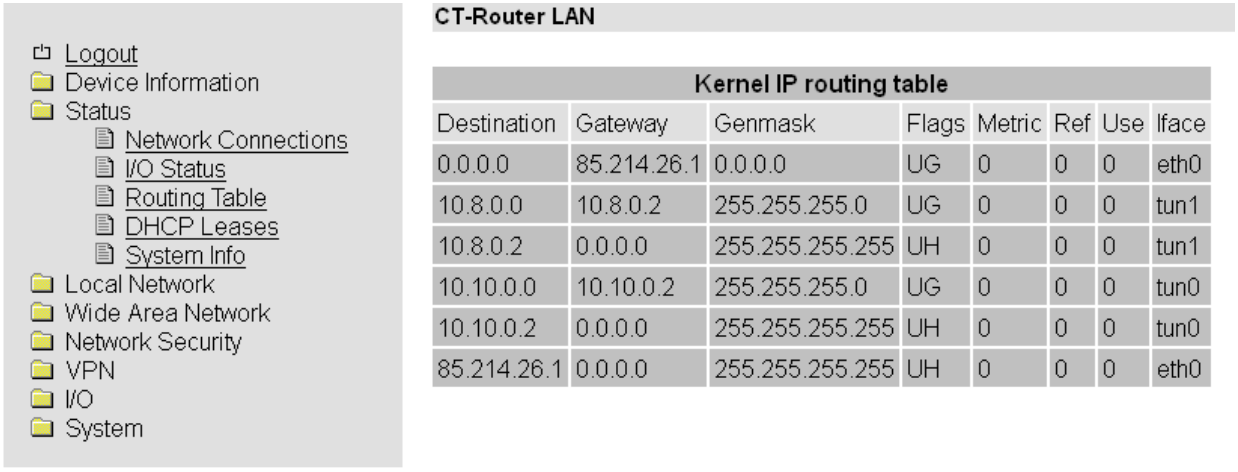
Status

I/O Status



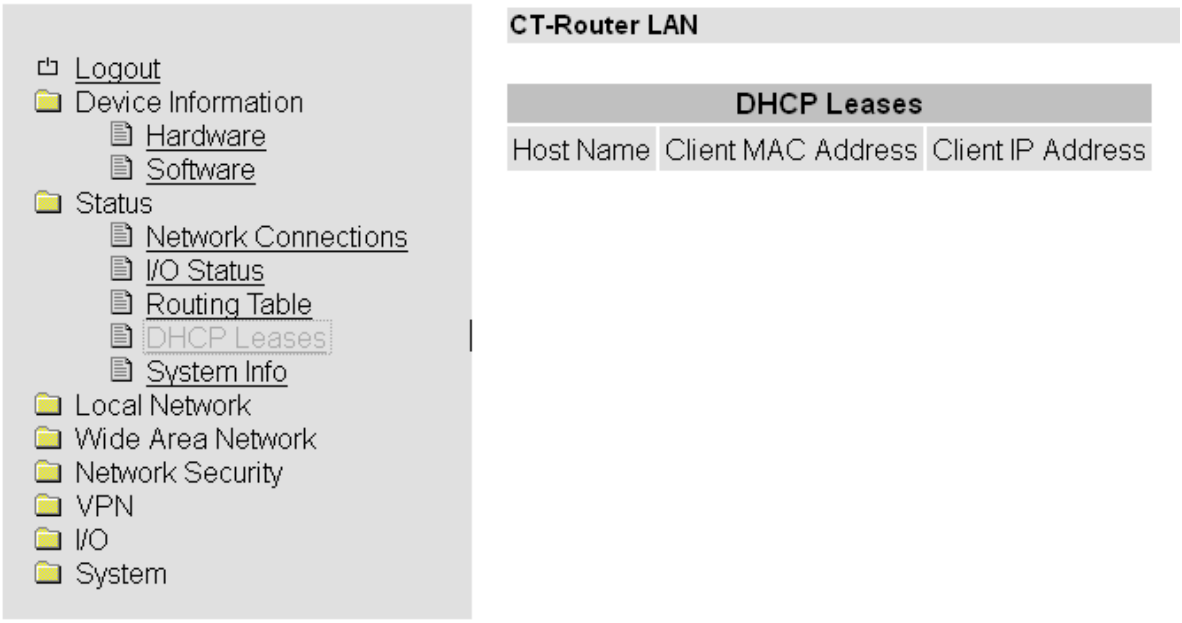
Tabellarische Übersicht aller aktuellen Input- und Outputeinstellungen.

Routing Table



Status →Routing Table	
Routing Table	Erklärung
Enthält unter anderem Informationen zum Ziel, Gateway, zur Subnetzmaske und Metrik.	

DHCP Leases

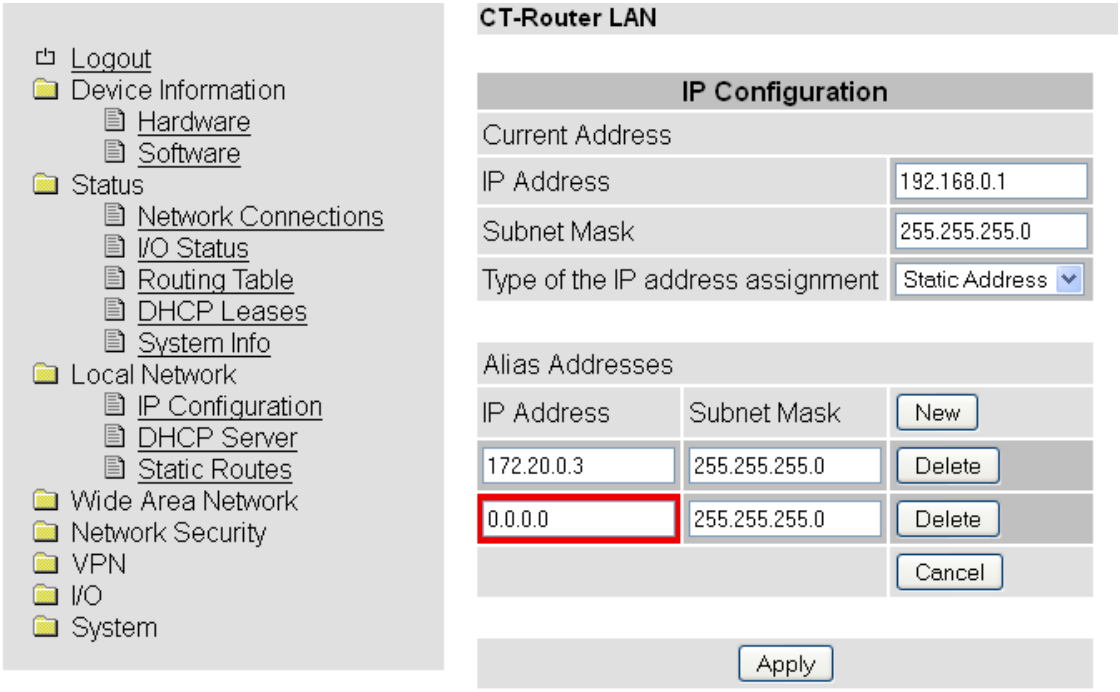


Status →DHCP Leases	
DHCP Leases	Erklärung
Tabellarische Übersicht aller vom CT-Router HSPA vergebenen DHCP-Daten.	
Host Name	Hostname des im Netzwerk befindlichen Endgerätes
Client MAC Address	MAC-Adresse des im Netzwerk befindlichen Endgerätes
Client IP Address	IP-Adresse des im Netzwerk befindlichen Endgerätes

Local Network

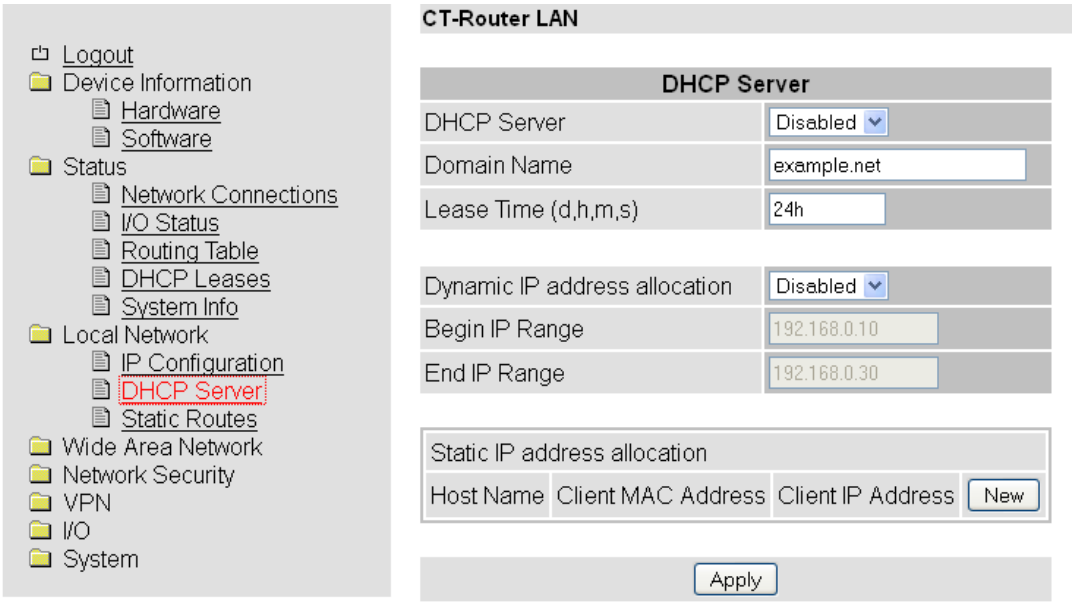
Im Menü „Local Network“ können Sie die lokale Netzwerkeinstellung für den CT-Router HSPA vornehmen. Ihre Einstellungen werden gespeichert, sind aber noch nicht gültig. Zur Übernahme der Einstellungen starten Sie den Router neu.

IP Configuration



Local Network → IP Configuration	
IP Configuration	**Erklärung**
Current Address	
IP Address	aktuelle IP-Adresse des Routers
Subnet Mask	Subnetzmaske der aktuellen IP-Adresse
Type of the IP address assignment	**Static:** Statische IP-Adresse (Standardeinstellung) **DHCP:** Dynamische IP-Adresse, wird beim Start des Routers von einem DHCP-Server bezogen
Alias Addresses	Max. 8 zusätzliche IP-Adressen sowie Subnetzmasken zuweisbar.
IP Address	alternative IP-Adresse des Routers
Subnet Mask	alternative Subnetzmaske des Routers

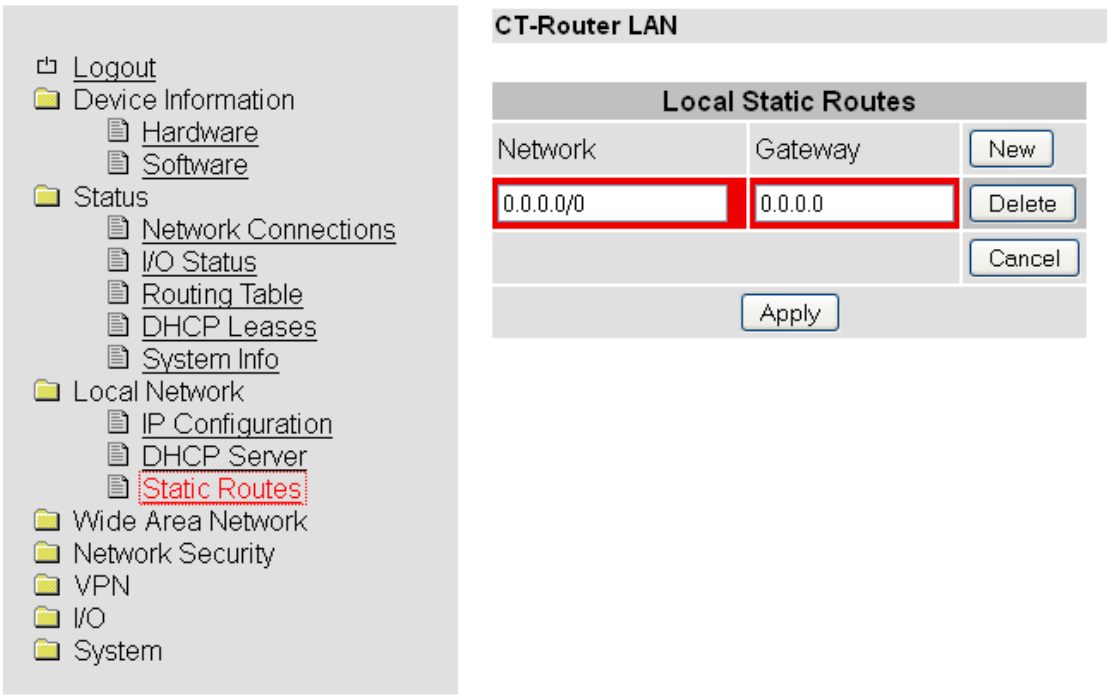
DHCP Server



Local Network → DHCP Server	
DHCP Server	**Erklärung**
DHCP Server	Deaktiviert / Aktiviert
Domain Name	Domain-Namen eintragen, der über DHCP verteilt wird.
Lease Time (d,h,m,s)	Zeitraum, in dem die Netzwerkkonfigurationen gültig sind.
Dynamic IP address allocation	Dynamische IP-Adressen-Zuweisung: Bei Aktivierung können Sie die entsprechenden Netzwerkparameter eintragen / Der DHCP-Server vergibt IP-Adressen aus dem angegeben IP-Bereich.
Begin IP Range	IP-Bereichsanfang
End IP Range	IP-Bereichsende
Static IP address allocation	IP-Adressen werden MAC-Adressen eindeutig zugeordnet.
Client MAC Address	MAC-Adresse des verbundenen Endgerätes
Client IP Address	IP-Adresse des verbundenen Endgerätes IP-Adressen dürfen nicht aus den dynamischen IP-Adressen Zuweisungen stammen. Eine IP-Adresse darf nicht mehrfach zugeordnet werden, da sonst einer IP-Adresse mehreren MAC-Adressen zugewiesen wird.

Local Network

Static Routes

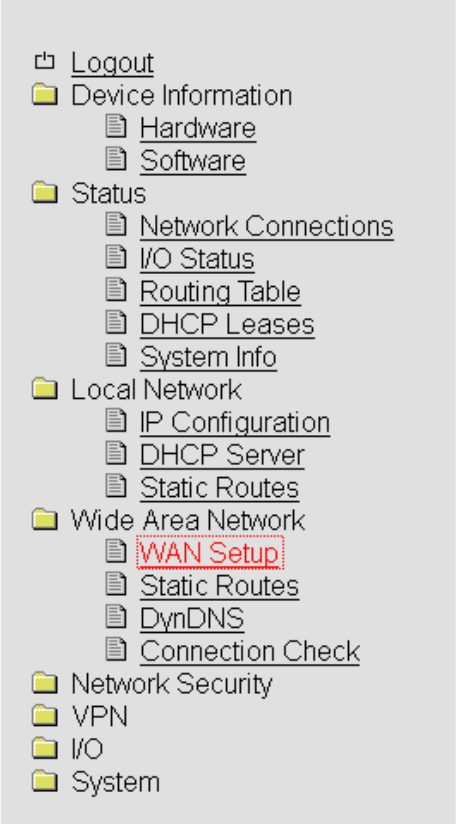


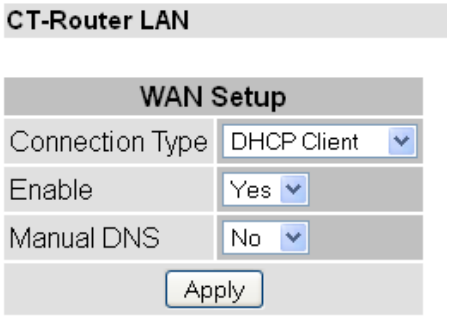
Local Network → Static Routes	
Static Routes	Erklärung
Network	Netzwerk in CIDR-Form
Gateway	Gateway-Adresse des Netzwerkes
Max. 8 Netzwerke eintragbar.	

Wide Area Network

Im “ Wide Area Network”-Menü legen Sie die Einstellungen des Routers für die Nutzung im WAN fest.

WAN Setup





Wide Area Networks	
WAN Setup	Erklärung
Connection Type	Wählen die Verbindungsart im Menü „Connection Type“ aus und setzen sie Enable auf „Yes“. Klicken Sie anschließend auf „Apply“

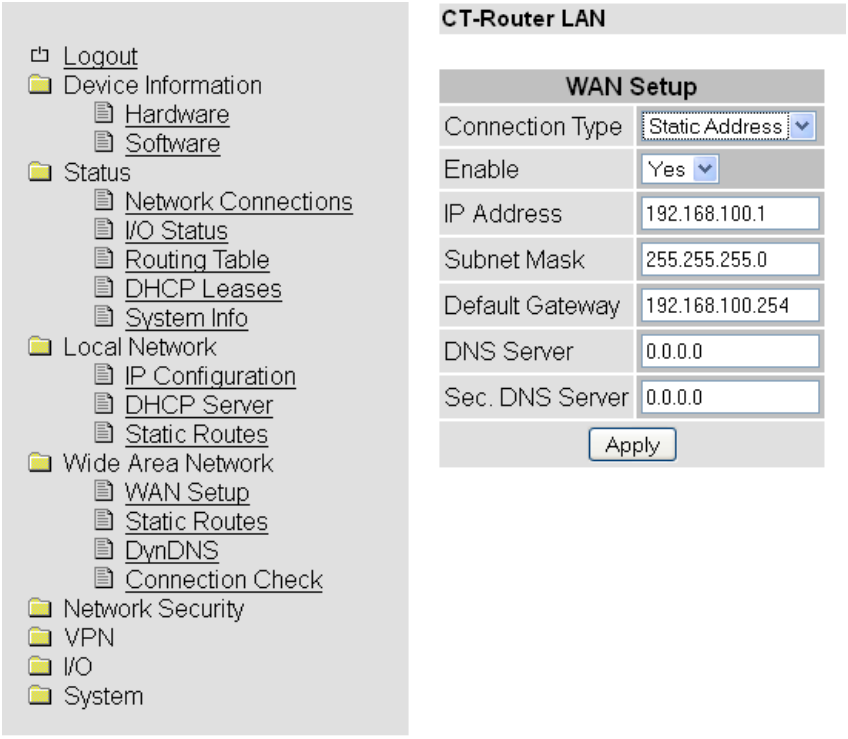
Mögliche Verbindungsarten im Menü „Connection Type“

- Static Address
- DHCP Client
- PPOE

Static Address

Einstellung für den Betrieb in lokalen Netzwerken

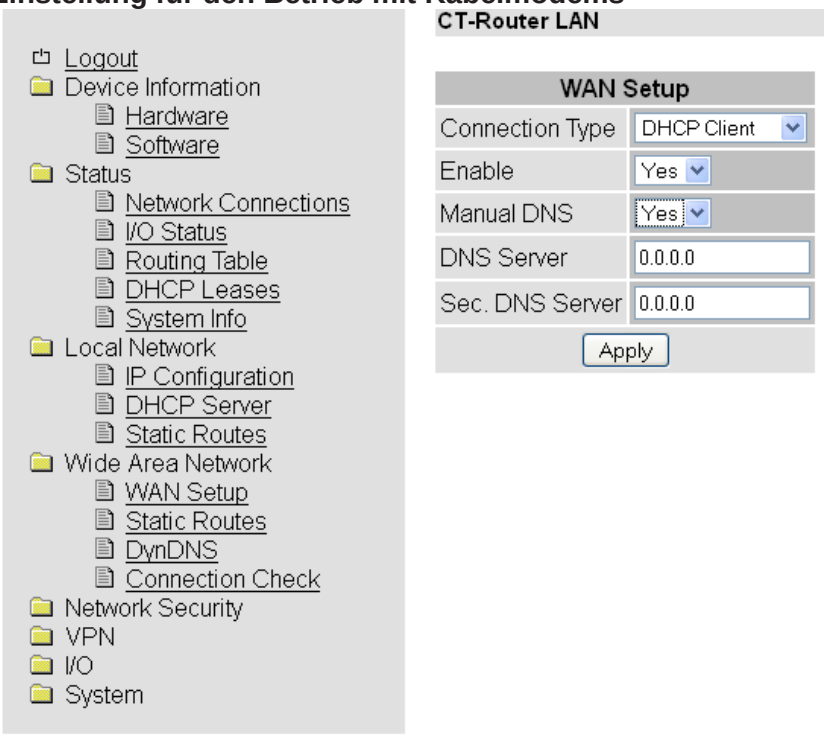
So könne Sie dem Router beim Betrieb in einem vorhandenen Netzwerk eine feste IP-Adresse zuteilen.



Wide Area Networks	
WAN Setup	Erklärung
IP Address	IP-Adresse des Routers an der WAN-Schnittstelle
Subnet Mask	Subnetzmaske
Default Gateway	IP-Adresse des Gateways in das Internet
DNS Server	IP-Adresse des DNS Servers
Sec. DNS Server	IP-Adresse eines zweiten DNS Servers

DHCP Client

Einstellung für den Betrieb mit Kabelmodems



Soll dem Router aus dem Netzwerk automatisch eine IP-Adresse zugewiesen werden setzen Sie den „Connection Type“ auf „DHCP Client“ und bestätigen mit „Apply“.

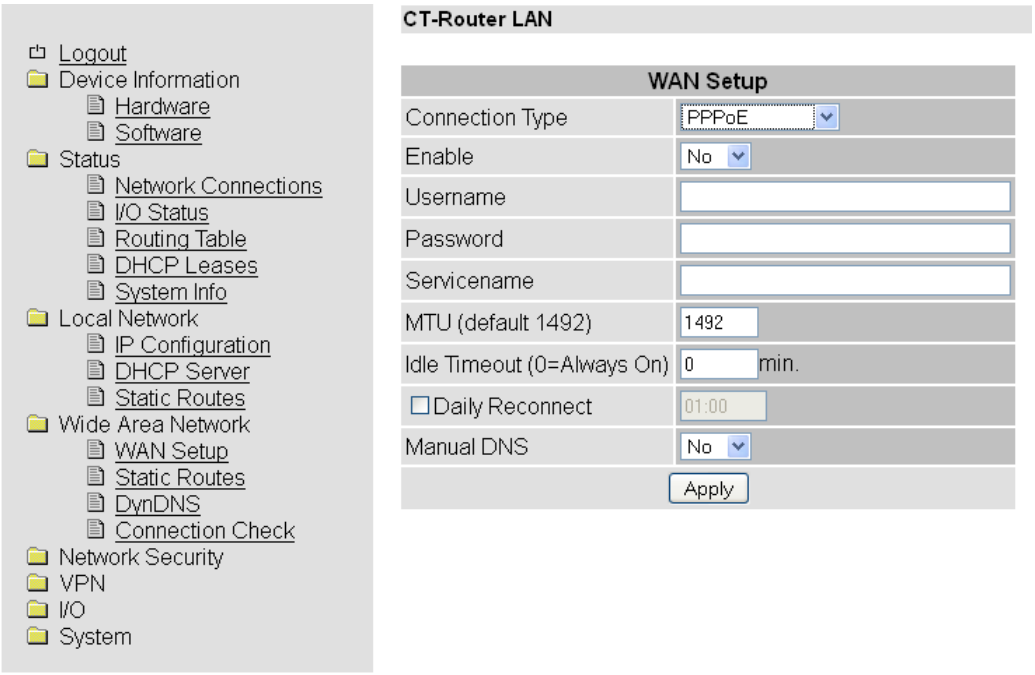
Wenn Sie die IP-Adressen des DNS-Servers manuell einstellen wollen setzen Sie unter „Manual DNS“ die Einstellung „Yes“ und geben die IP-Adressen ein und klicken abschließend auf „Apply“.

Wide Area Networks	
WAN Setup	Erklärung
DNS Server	IP-Adresse des DNS Servers
Sec. DNS Server	IP-Adresse eines zweiten DNS Servers

PPPoE

Einstellung für den Betrieb mit DSL-Modems

Bei einen Betrieb an einem (DSL-)Modem wählen Sie unter „Connection Type" die Einstellung „PPPoE" und mit „Apply" bestätigen

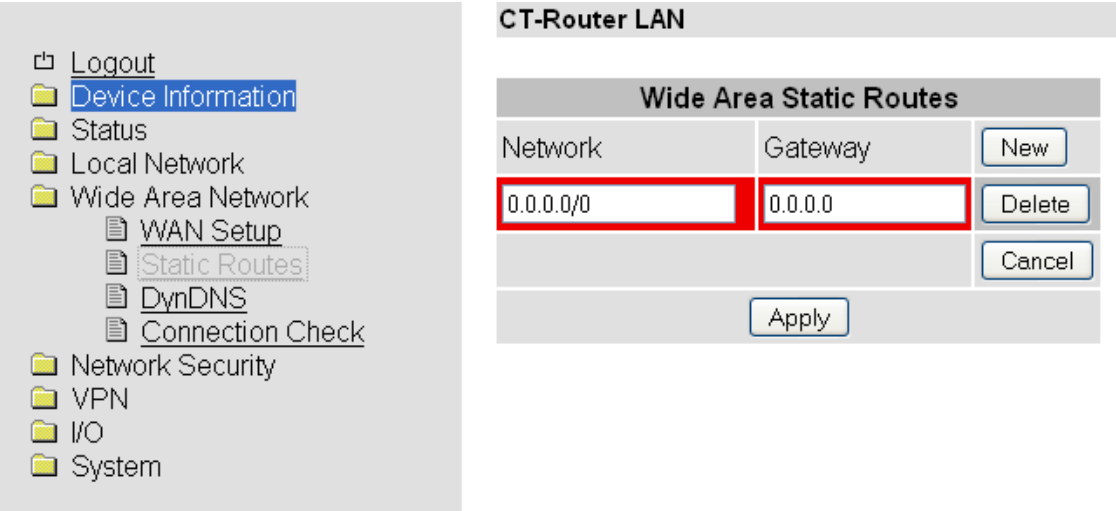


Wide Area Networks	
WAN Setup	**Erklärung**
Username	Username für den Zugang zum Netz
Password	Password für den Zugang zum Netz
Servername	Service-Name für den Zugang (DSL-) Netz
MTU (default 1492)	Maximale Größe der unfragmentierten Datenpakets
Idle Timeout (0=Always On)	Der Router trennt die Verbindung nach der eingestellten Zeit. Der Timer startet wenn keine Daten übertragen mehr werden.
Daily Reconnect	Wiederholtes Einbuchen in das (DSL-)Netz zu einer definierten Uhrzeit
Manual DNS	Yes: Manuelle Einstellung No: Keine manuelle Einstellung

Wide Area Network

Static Routes

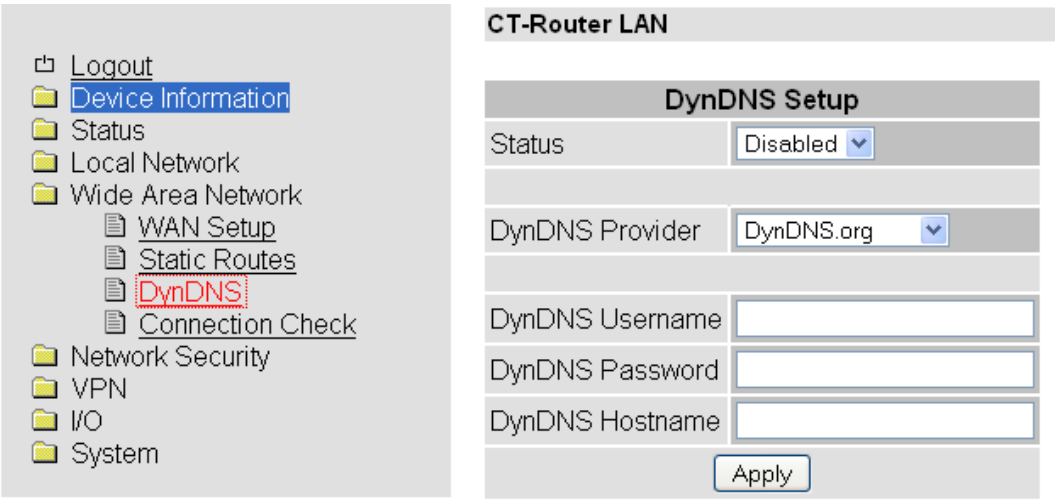
Per „Static Routes“ können Datenpakete aus dem lokalen Netzwerk für alternative Routen im WAN festgelegt werden.



Wireless Network → Static Routes	
Static Routes	Erklärung
Network	Netzwerk in CIDR-Form
Gateway	Gateway-Adresse des Netzwerkes
Max. 8 Netzwerke möglich	

DynDNS

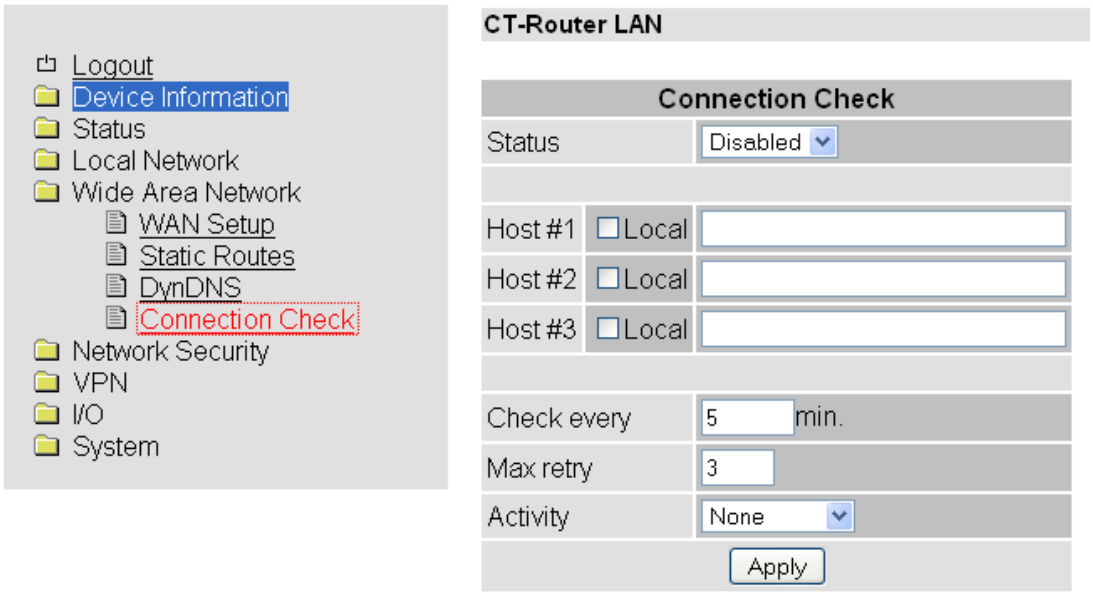
Die IP-Adresse des Routers im Internet wird dynamisch von dem Netzbetreiber zugewiesen.
Über einen DynDNS-Anbieter kann der dynamischen IP-Adresse ein Name zugewiesen werden, über die der Router
dann über das Internet erreicht werden kann. Auf dem Router muss entsprechend der DynDNS Client angelegt und aktiviert werden.



Wireless Network → DynDNS	
DynDNS	Erklärung
DynDNS	**Disable:** Deaktivierung der DynDNS **Enable:** Aktivierung der DynDNS
DynDNS Provider	Auswahl des DynDNS-Anbieters
DynDNS Username	Benutzername des DynDNS-Accounts
DynDNS Password	Passwort des DynDNS-Accounts
DynDNS Hostname	Hostname des Routers beim DynDNS-Service

Connection Check

Eine kontinuierliche Verbindungsüberwachung kann durch den „Connection Check" überprüfen, ob die Daten-Verbindung zum Internet besteht. Bei einem Verbindungsverlust kann für einen neuen Verbindungsaufbau eine Aktion konfiguriert werden.

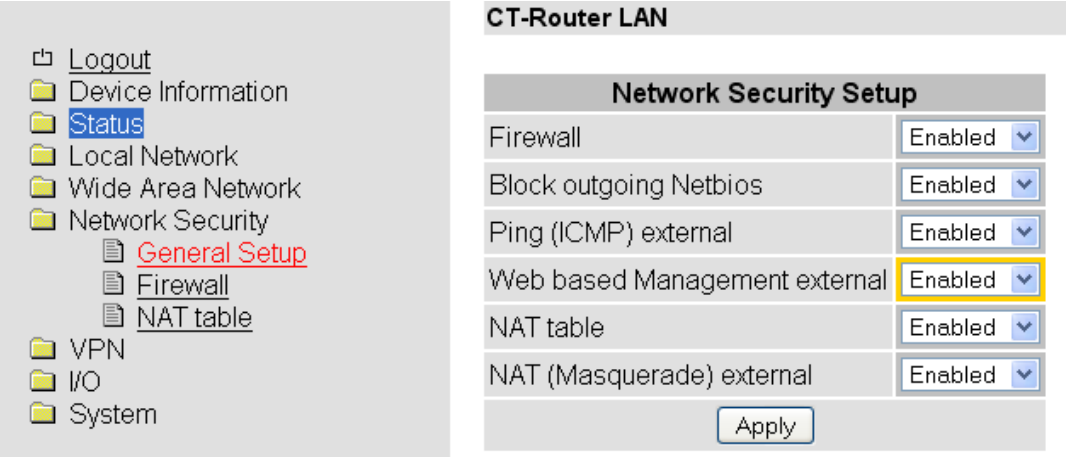


Wireless Network → Connection Check	
Connection Check	**Eklärung**
Connection Check	**Disable:** Deaktivierung der Verbindungsprüfung der Paketdaten-Verbindung **Enable:** Aktivierung der Verbindungsprüfung der Paketdaten-Verbindung
Host #1…#3	IP-Adresse oder Hostnamen als Referenzpunkt zur Verbindungsprüfung **Local:** Aktivierung bei Adressen, die über einen VPN-Tunnel erreichbar sind
Check every	Es wird alle x Minuten die Verbindung geprüft.
Max. retry	Maximale Anzahl der Verbindungsversuche
Activity	Bei Verbindungsabbruch eine der folgenden Aktionen ausführen: **Reboot:** Router Neustart **Reconnect:** Verbindung wird versucht neu aufzubauen **Relogin:** Mobilfunkinterface wird heruntergefahren und erneuter Versuch eines Verbindungsaufbaus mit Login. **None:** keine Aktion wird ausgeführt

Network Security

In diesem „Network Security”-Menü nehmen Sie Einstellungen zu Netzwerksicherheit vor.

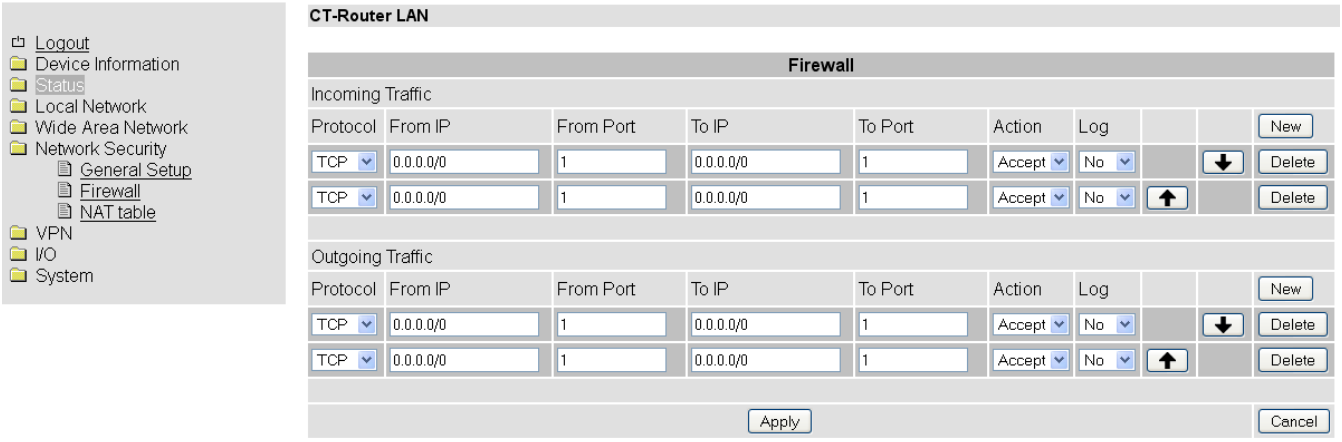
General Setup



Network Security → General Setup	
General Setup	Erklärung
Firewall	**Disable:** Deaktivierung der integrierten Stateful Packet Inspection Firewall **Enable:** Aktivierung der integrierten Stateful Packet Inspection Firewall
Block outgoing Netbios	Netbios-Anfragen gehen von Windows-Systemen im lokalen Netzwerk aus und verursachen einen erhöhten Datenverkehr. **Disable:** Netbios-Anfragen werden erlaubt **Enable:** Netbios-Anfragen werden geblockt
Ping (ICMP) external	Ping-Anfragen prüfen, ob ein Gerät im Netzwerk erreichbar ist. Dadurch erhöht sich der Datenverkehr. **Disable:** Ping-Anfragen aus dem externen IP-Netz werden nicht beantwortet **Enable:** Ping-Anfragen aus dem externen IP-Netz werden beantwortet
Web based Management external	**Disable:** Externe WBM Konfiguration ist deaktiviert **Enable:** Externe WBM Konfiguration ist aktiviert
NAT (Masquerade) external	**Disable:** IP-Masquerading deaktiviert **Enable:** IP-Masquerading aktiviert

Firewall

Die Firewall ist ein- und ausschaltbar. Die Firewall ist per default aktiv und blockiert den eingehenden Datenverkehr. Der ausgehende Datenverkehr ist aber möglich. Die Firewall-Regeln werden von oben nach unten angewendet.

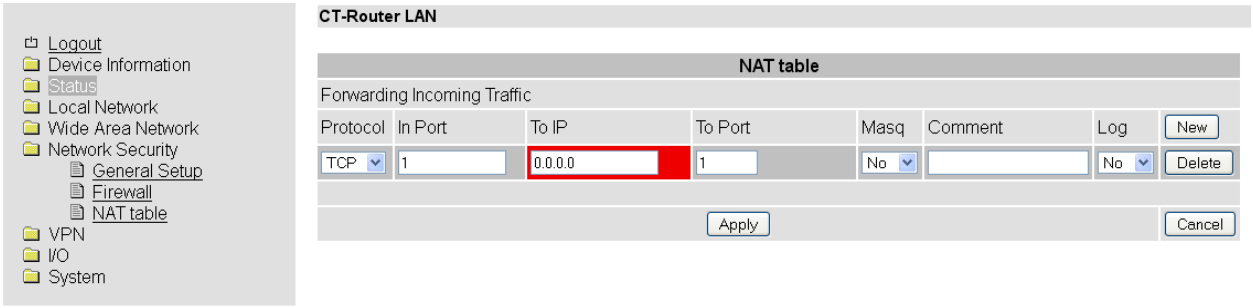


Network Security → Firewall	
Firewall	**Erklärung**
Incoming Traffic	
Protocol	Protokollauswahl: TCP, UDP, ICMP, all
From IP / To IP	IP-Adressenbereich in CIDR-Form (0.0.0.0/0 bedeutet alle IP-Adressen)
From Port / To Port	bei TCP und UDP haben Sie folgende Optionen: direkte Port-Angabe z.B: From Port = 20, To Port = 30 Portbereiche z.B: From Port oder To Port = 80-89 (alle Ports von 80-89) Portbereich "any" bezeichnet alle Ports
Action	**Accept:** Datenpakete werden angenommen. **Reject:** Datenpakete werden abgelehnt. Benachrichtigung an den Absender, dass die Daten abgelehnt werden. **Drop:** Datenpakete werden "fallen gelassen" d.h. sie werden abgewiesen und der Absender erhält keine Benachrichtigung.
Log	**Yes:** Aktivierung der Regel wird protokolliert **No:** Aktivierung der Regel wird nicht protokollier.
New / Delete	Neue Regel aufstellen / bestehende Regel löschen
	Mit den Pfeilen können Regeln nach oben oder unten verschoben werden.
Outgoing Traffic	Verhält sich ähnlich zum „Incoming Traffic“, jedoch beziehen sich diese Regeln auf den ausgehenden Datenverkehr. Ist keine Regel vorhanden, so sind alle ausgehenden Verbindungen verboten (mit Ausnahme von VPN-Verbindungen)

Network Security

NAT Table

Der Router hat nur eine IP-Adresse, über die von außen auf ihn zugegriffen werden kann.
Über zusätzlich übermittelte Portnummern können Datenpakete auf Ports interner IP-Adressen umgeleitet werden



Network Security →NAT Table	
Firewall	**Erklärung**
Protocol	Protokollauswahl: TCP, UDP, ICMP, all
In Port / To Port	bei TCP und UDP haben Sie folgende Optionen: direkte Port-Angabe z.B: In Port = 20, To Port = 30 Portbereiche z.B: In Port = 80-89 To Port= 110-120
To IP	IP-Adressenbereich in CIDR-Form (0.0.0.0/0 bedeutet alle IP-Adressen)
Masq	**Yes:** IP-Masquerading aktiviert / Antwort ins Netz möglich **No:** IP-Masquerading deaktiviert / Antwort ins Netz nicht möglich
Log	**Yes:** Aktivierung der Regel wird protokolliert **No:** Aktivierung der Regel wird nicht protokolliert
New / Delete	Neue Regel aufstellen / bestehende Regel löschen
	Mit den Pfeilen können Regeln nach oben oder unten verschoben werden.

VPN

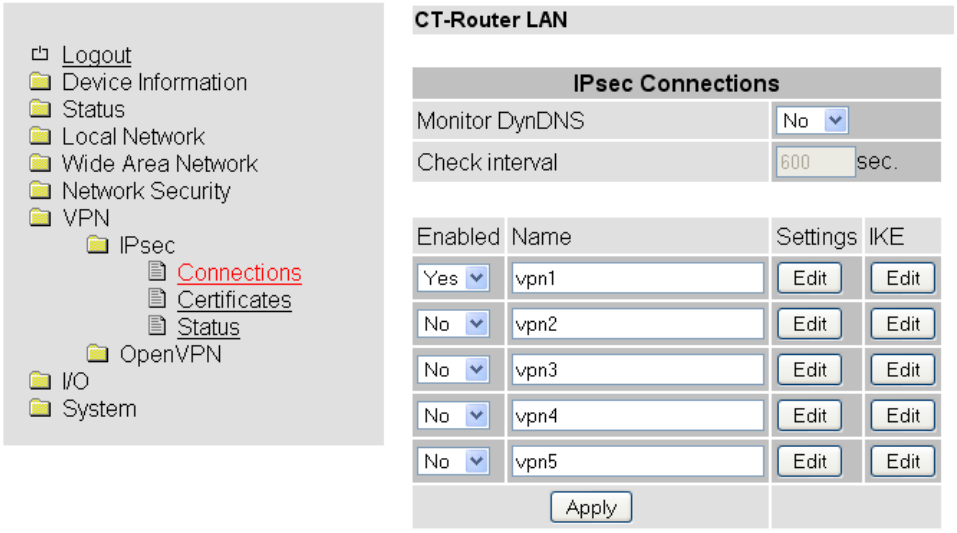
Im Menü VPN können Sie einerseits Einstellungen zur Internet Protocol Security (IPsec) andererseits zum virtuellen privaten Netzwerk (OpenVPN) vornehmen.

Für eine VPN-Verbindung müssen die IP-Adressen der VPN-Gegenstellen bekannt und adressierbar sein. Die VPN-Gegenstelle muss IPsec mit folgender Konfiguration unterstützen:

- Authentifizierung über X.509-Zertifikate oder Preshared Secret Key (PSK)
- ESP
- Diffie-Hellman Gruppe 2 oder 5
- 3DES oder AES encryption
- MD5 oder SHA-1 Hash Algorithmen
- Tunnel-Modus
- Quick Mode
- Main Mode
- SA Lifetime (1 Sekunde bis 24 Stunden)

IPsec

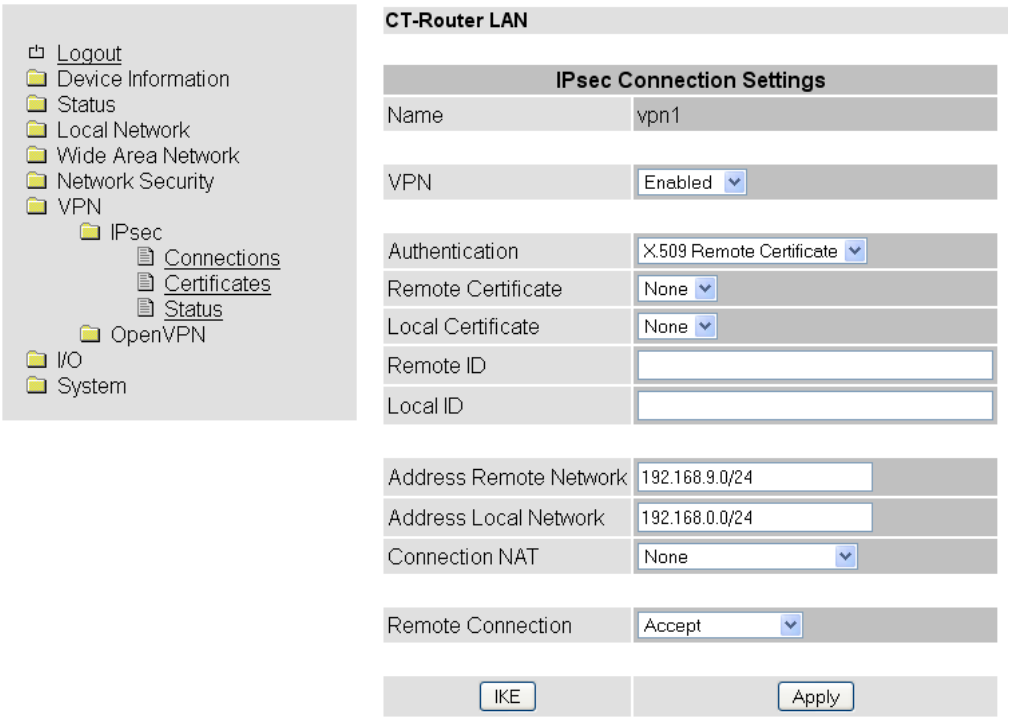
Connections



VPN → IPsec → Connections	
IPsec Connections	**Erklärung**
Monitor DynDNS	VPN-Gegenstelle hat keine feste IP und als Remote Host wird ein DynDNS-Name genutzt, so kann diese Funktion aktiviert werden, um die Verbindung zu überprüfen.
Check Interval	Prüfintervall in Sekunden
Enable	VPN-Verbindung aktivieren (=Yes) oder deaktivieren (=No)
Name	Name der VPN-Verbindung festlegen
Settings	Einstellungen für IPsec
IKE	Einstellungen für das Internet-Key-Exchange-Protokoll

IPsec

Connections Settings

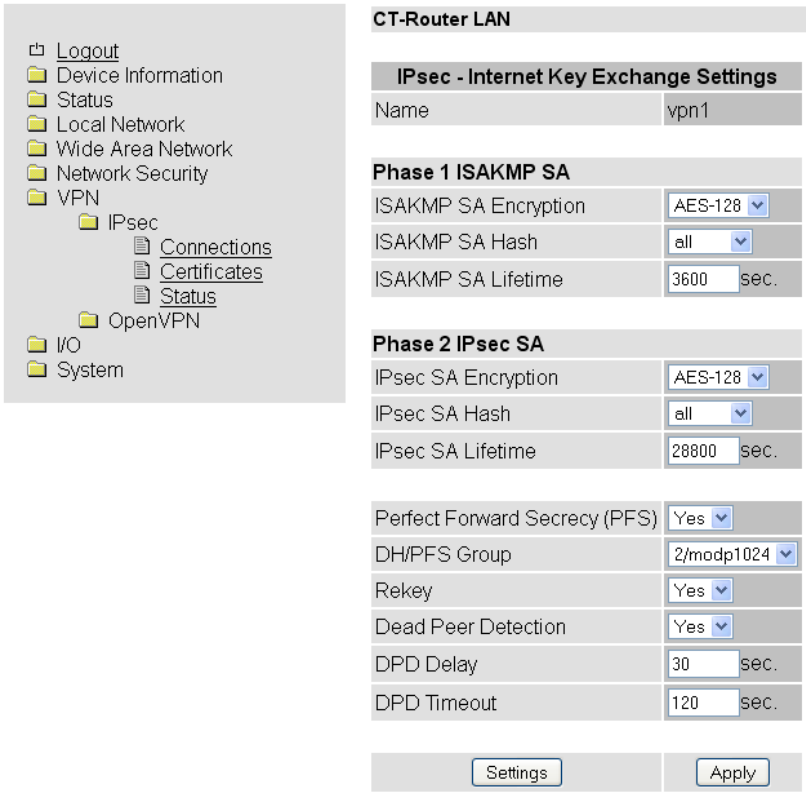


VPN → IPsec → Connections → Settings → Edit	
Settings	**Erklärung**
Name	Name der VPN-Verbindung
VPN	Aktivieren (=Enable) oder Deaktivieren (=Disable) der VPN-Verbindung
Remote Host	IP-Adresse / URL der Gegenstelle Kann nur eingestellt werden, wenn unter Remote Connection "Initiate" ausgewählt wurde. Wurde unter Remote Connection "Accept" ausgewählt, so wird der Wert für Remote Host auf "%any" gesetzt, und es wird auf eine Verbindung gewartet.
Authentication	X.509 Remote Certificate - VPN-Teilnehmer haben einen privaten und einen öffentlichen Schlüssel (X.509-Zertifikat). Preshared Secret Key - VPN-Teilnehmer besitzen einen privaten Schlüssel (ein gemeinsames Passwort).
Remote Certificate	VPN-Gegenstellen Authentifizierung erfolgt über ein Zertifikat, das in dem Menü "IPsec Certificates" hochgeladen werden muss.
Local Certificate	Router Authentifizierung bei der VPN-Gegenstelle erfolgt über ein Zertifikat, das in dem Menü "IPsec Certificates" hochgeladen werden muss.

IPsec

Remote ID	**Leer:** Kein Eintrag in der Zeile bedeutet, dass die Angaben aus dem Zertifikat gewählt werden. **Subject:** Eine IP-Adresse, E-Mail-Adresse oder ein Hostname bedeutet, dass diese Einträge auch im Zertifikat vorhanden sein sollten, damit sich der Router authentifizieren kann.
Local ID	Siehe Remote ID
Address Remote Network	IP-Adresse/Subnetzmaske des Netzwerkes, zu dem eine VPN-Verbindung aufgebaut wird.
Address Local Network	IP-Adresse/Subnetzmaske vom lokalen Netzwerk.
Local 1:1 NAT	IP-Adresse vom lokalen Netzwerk, unter der das Netzwerk per 1:1 NAT aus dem Remote-Netz erreicht werden kann/soll.
Remote Connection	**Accept:** VPN-Verbindung wird von einer Gegenstelle aufgebaut und vom Router akzeptiert. **Initiate:** VPN-Verbindung geht vom Router aus. **Initiate on Input:** Startet / Stoppt den VPN-Tunnel durch digitalen Eingang. **Initiate on SMS:** VPN-Verbindung wird durch eine SMS gestartet **Initiate on Call:** VPN-Verbindung wird durch einen Anruf gestartet
Autoreset	Kann bei "Initiate on SMS" und muss bei "Initiate on Call" festgelegt werden. Es wird ein Zeitraum festgelegt, nach wieviel Minuten die VPN-Verbindung per Autoreset gestoppt wird.

Connection IKE



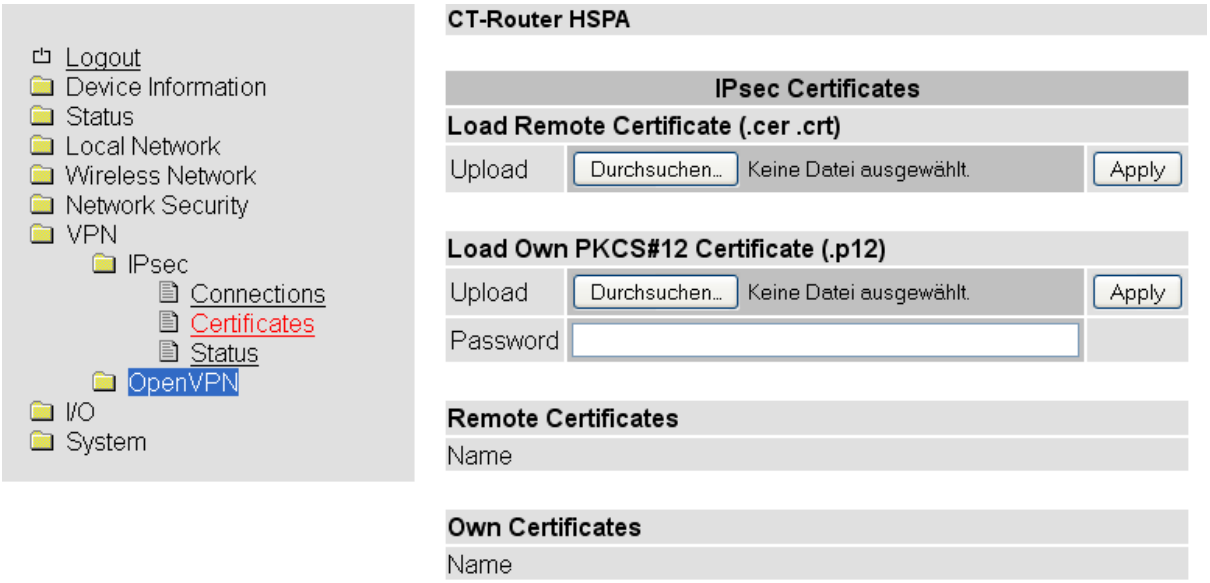
VPN → IPsec → Connections → IKE → Edit	
IKE	Erklärung
Name	Name der VPN-Verbindung.
Phase 1 ISAKMP SA	Schlüsselaustausch
ISAKMP SA Encryption	Verschlüsselungsalgorithmus-Auswahl
ISAKMP SA Hash	Hash-Algorithmus-Auswahl
ISAKMP SA Lifetime	Lebensdauer des ISAKMP SA Schlüssels. Standardeinstellung 3600 Sekunden (1 Stunde) max. Einstellwert 86400 Sekunden (24 Stunden)
Phase 2 IPsec SA	Datenaustausch
Ipsec SA Encryption	siehe ISAKMP SA Encryption
Ipsec SA Hash	siehe ISAKMP SA Hash
Ipsec Lifetime	Lebensdauer des Ipsec SA Schlüssels. Standardeinstellung 28800 Sekunden (8 Stunden) max. Einstellwert 86400 Sekunden (24 Stunden)
Perfect Forward Secrecy (PFS)	Aktivieren (=Yes) oder Deaktivieren (=No) der PFS Funktion.

IPsec

DH/PFS Group	Im Ipsec werden beim Datenaustausch in bestimmten Intervallen die Schlüssel erneuert. Mit PFS werden hierbei mit der Gegenstelle im Schlüsselaustauschverfahren neue Zufallszahlen ausgehandelt.
Dead Peer Detection	Auswahl des Verfahrens. **Yes:** Bei VPN Initiate wird versucht, neuzustarten "Restart. Bei VPN Accept wird die Verbindung geschlossen "Clear".
DPD Delay (sec.)	Zeitintervall in Sekunden, in dem die Peer-Verbindung überprüft wird.
DPD Timeout (sec.)	Zeitspanne in Sekunden nach der ein Timeout erfolgen soll.

Certificates

Mit einem Zertifikat, das in den Router geladen werden kann, authentifiziert sich der Router bei der Gegenstelle.

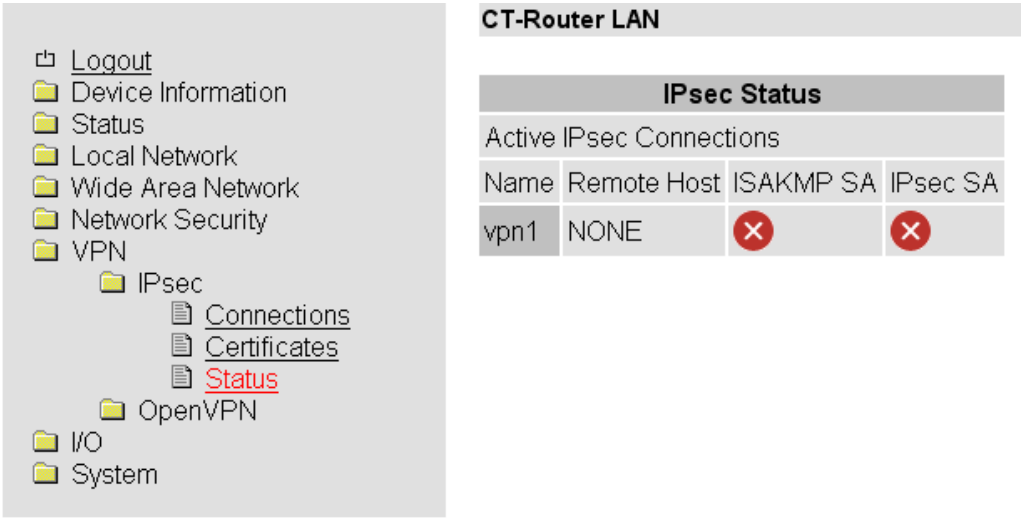


Durch Klicken auf „Apply“ laden Sie das Zertifikat auf den Router.

VPN → IPsec → Certificates	
Certificates	**Erklärung**
Load Remote Certificate	Hochladen von Zertifikaten, mit denen eine Authentifizierung für den Router bei der VPN-Gegenstelle erfolgen kann.
Load Own PKCS#12 Certificate	Hochladen eines Zertifikats (Providervorgabe)
Password	Passwort für das PKCS#12 Zertifikat / das Passwort wird beim Export vergeben
Remote Certificates	Tabellarische Übersicht aller "Remote Certificates" / mit "Delete" wird ein Zertifikat gelöscht
Own Certificates	Tabellarische Übersicht aller "Own Certificates" / mit "Delete" wird ein Zertifikate gelöscht

IPsec

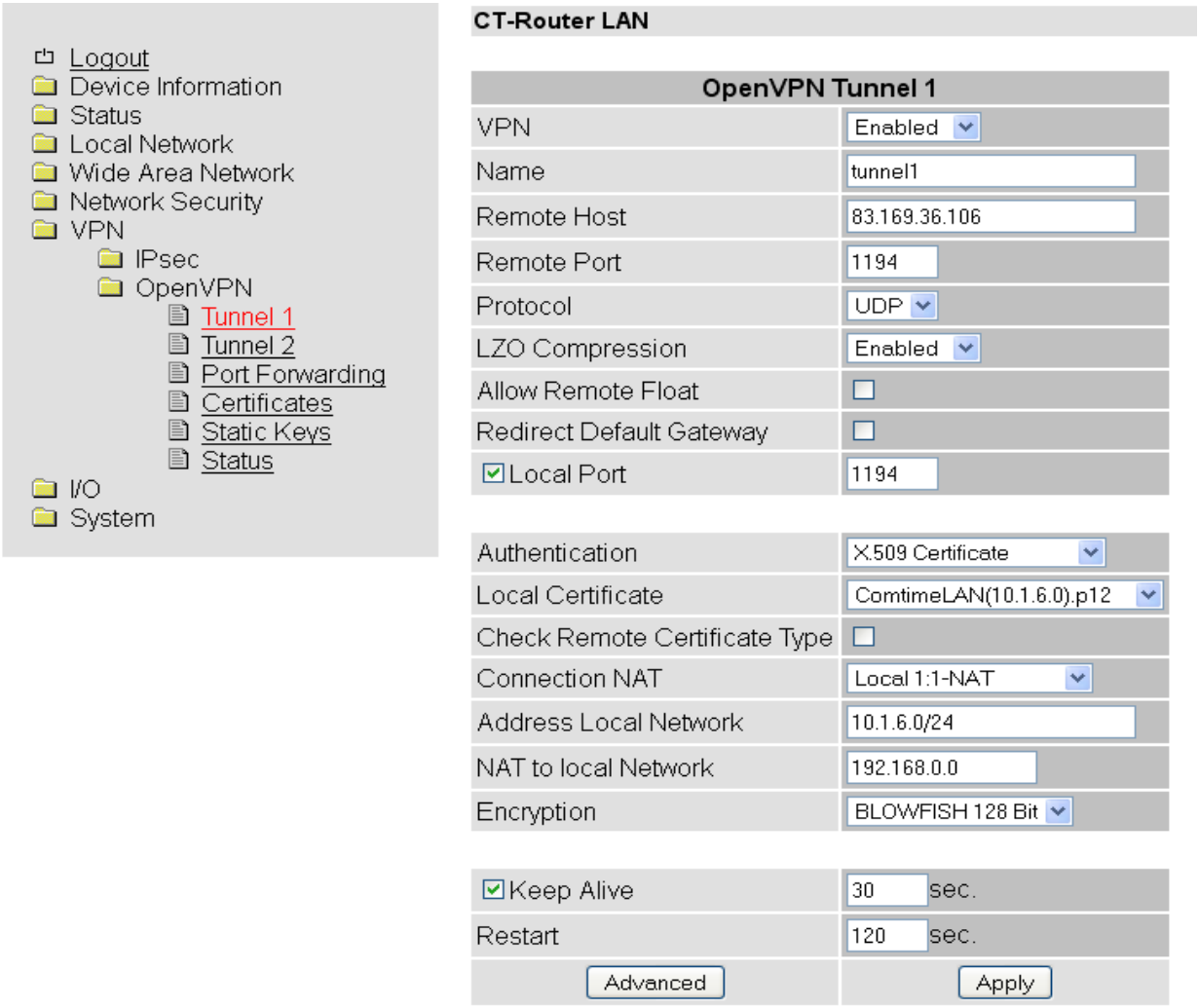
Status



VPN → IPsec → Status	
Status	Erklärung
Name	Name der VPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
ISAKMP SA	Aktiv (grünes Feld)
IPSec SA	Aktiv (grünes Feld)

OpenVPN

Tunnel

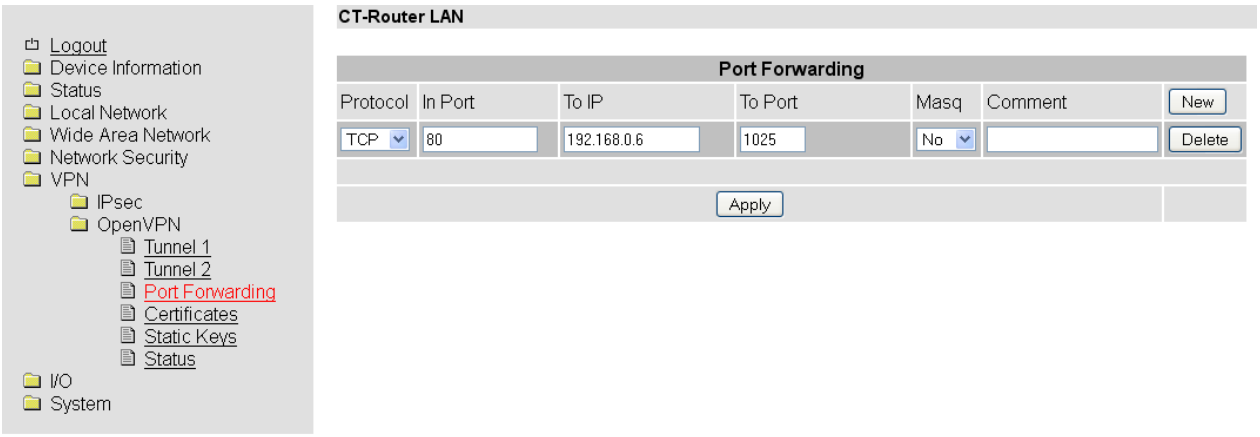


VPN → OpenVPN → Tunnel	
OpenVPN Tunnel	**Erklärung**
VPN	OpenVPN Tunnel aktiv (=Enable) oder inaktiv (=Disable)
Name	Name der OpenVPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
Remote Port	Port der Gegenstelle (Standard: 1194)
Protocol	UDP- oder TCP-Protokoll für die OpenVPN-Verbindung festlegen!
LZO Compression	**Disabled:** Keine Kompression **Adaptive:** Adaptive Kompression **Yes:** Kompression aktiviert

OpenVPN

Allow Remote Float	Option: Bei der Kommunikation mit dynamischen IP-Adressen akzeptiert die OpenVPN-Verbindung authentifizierte Pakte von jeder IP-Adresse.
Local Port	Lokaler Port
Authentication	Authentifizierungsart der OpenVPN-Verbindung festlegen (X.509 oder PSK)!
Local Certifacation	Zertifikat vom Router für die Authentifizierung bei der Gegenstelle
Check Remote Certificate Type	Option: Zertifikate der OpenVPN-Verbindung überprüfen
Address Local Network	IP-Adresse/Subnetzmaske des lokalen Netzwerks
Local 1:1 NAT	Option: IP-Adresse vom lokalen Netzwerk, unter der das Netzwerk per 1:1 NAT aus dem Remote-Netz erreicht werden kann/soll.
Encryption	Verschlüsselungsalgorithmus der OpenVPN-Verbindung
Keep Alive	Zeitintervall in Sekunden von Keep Alive-Anfragen an die Gegenstelle
Restart	Zeitspanne in Sekunden nach der die Verbindung neu gestartet werden soll, falls keine Antwort auf die Keep Alive-Anfragen erfolgt.

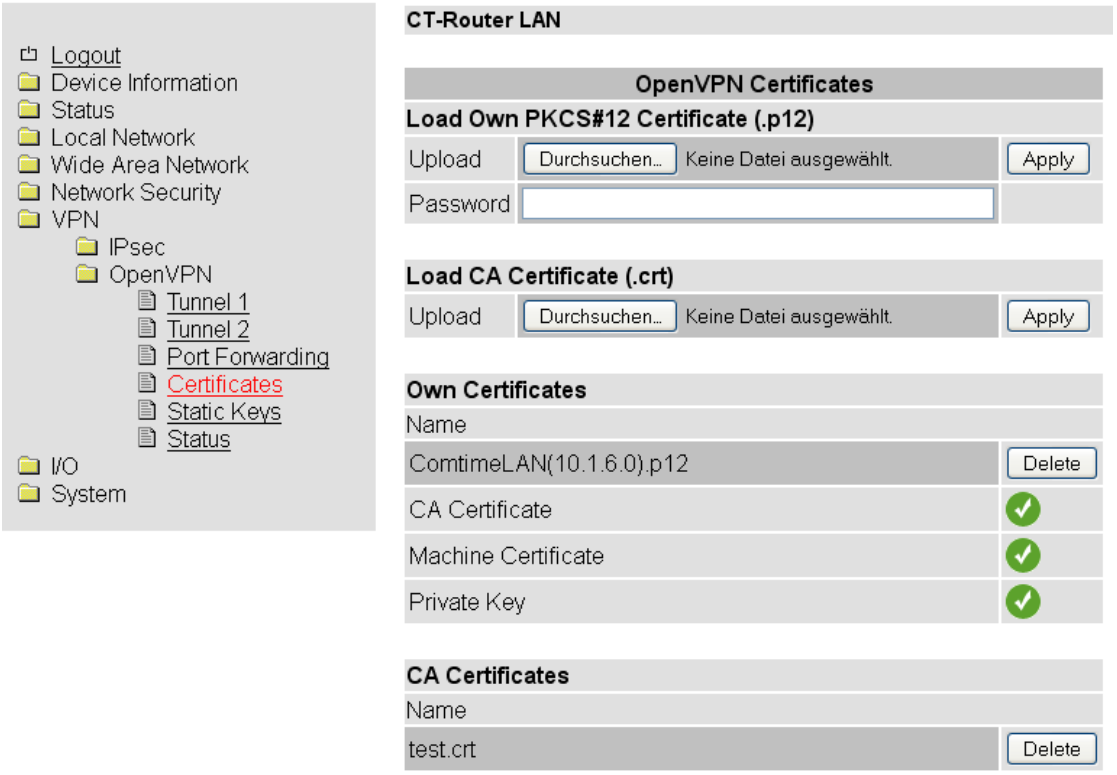
Port Forwarding



VPN → OpenVPN → Port Forwarding	
Port Forwarding	**Erklärung**
Protocol	Auswahl: TCP / UDP / ICMP
In Port	Port Nr. eingehende Verbindung
To IP	IP Adresse von Ziel
To Port	Port Nr. Vom Ziel

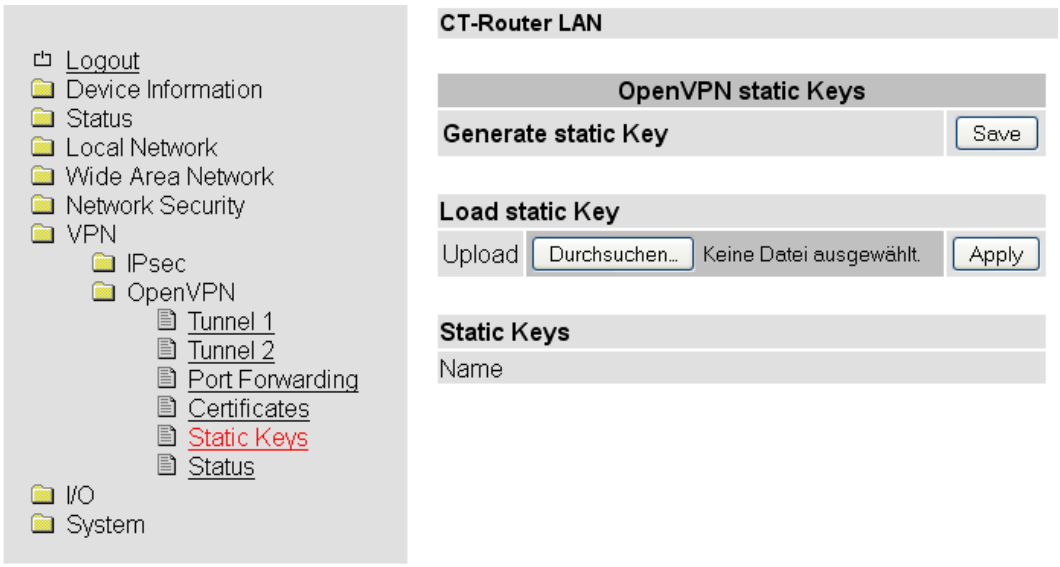
OpenVPN

Certificates



VPN → OpenVPN → Certificates	
Certificates	**Erklärung**
Load Own PKCS#12 Certificate	Hochladen des Zertifikats (im PKCS#12 Format, xxx.p12) welches für den Lokalen Router bestimmt ist. Unter VPN > OpenVPN > Client können Sie für jede VPN-Verbindung eines dieser Zertifikate unter Local Certificate zuweisen.
Password	Passwort für das PKCS#12 Zertifikat. Das Passwort wird beim Export vergeben.
Own Certificates	Tabellarische Übersicht aller "Own Certificates" / mit "Delete" werden die Zertifikate gelöscht

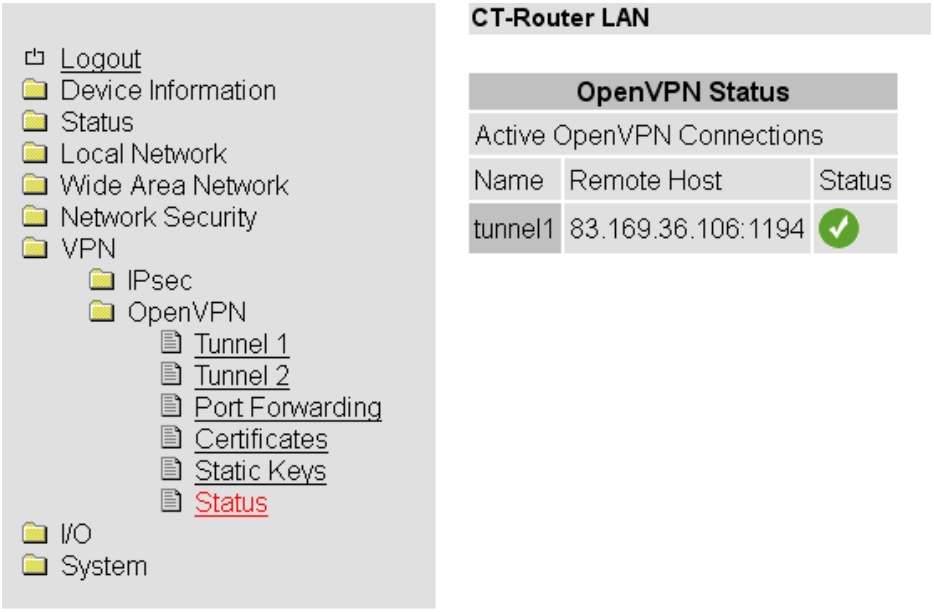
Static Keys



VPN → OpenVPN → Static Keys	
Static Keys	Erklärung
Generate static Key	Einen statischen Schlüssel generieren und speichern.
Load static Key	Statischen Schlüssel in den Router laden (den gleichen statischen Schlüssel muss auch die Gegenstelle besitzen).
Static Keys	Tabellarische Übersicht aller geladenen statischen Schlüssel.

OpenVPN

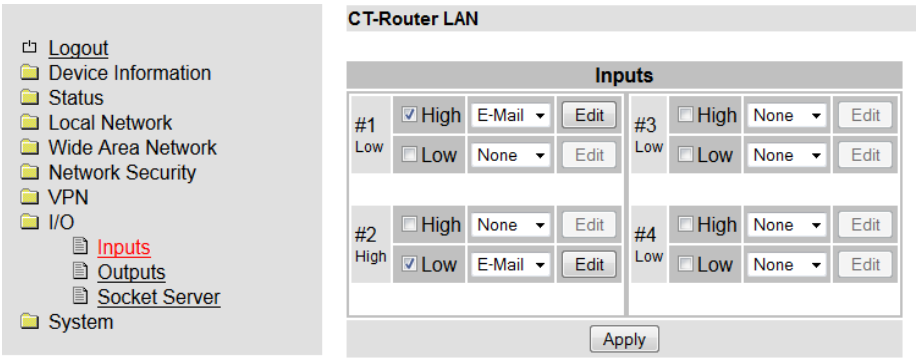
Status



VPN → OpenVPN → Status	
OpenVPN Status	Erklärung
Name	Name der VPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
Status	Aktiv (=grünes Feld)

Der Router LAN verfügt über vier digitale Ein- und Ausgänge, die in dem „I/O“-Menü von Ihnen konfiguriert werden können.

Inputs



I/O →Inputs	
Inputs	Erklärung
High	Option: Bei einem High-Pegel kann eine Nachricht per E-Mail verschickt werden.
Low	Option: Bei einem Low-Pegel kann eine Nachricht per E-Mail verschickt werden.
Stellt man nun eine der oben dargestellten Optionen ein, so muss man diese mit "Apply" bestätigen. Erst dann können die Einstellungen für die Benachrichtigung editiert werden. E-Mail: Sie können einen Empfänger, einen Kopie-Empfänger, einen Betreff und einen Nachrichtentext festlegen.	

Achtung: Bitte beachten Sie ob der Schalteingang bereits zum Starten einer IPsec VPN-Verbindung genutzt wird. In diesem Fall den Input nicht für das Versenden von E-Mail verwenden.

Für den Versand von E-Mails muss der E-Mail Account unter Punkt „SMTP Configuration“ eingerichtet worden sein

Schalteingänge anschließen

- Schließen Sie die Schalteingänge an den jeweiligen steckbaren Schraubklemmen an.
- An die Schalteingänge (I1 ... I4) können Sie 10 ... 30 V DC anschließen.
- Das 0-V-Potential der Schalteingänge müssen Sie an die "0 V" Klemme des Spannungs-Anschlusses anschließen.

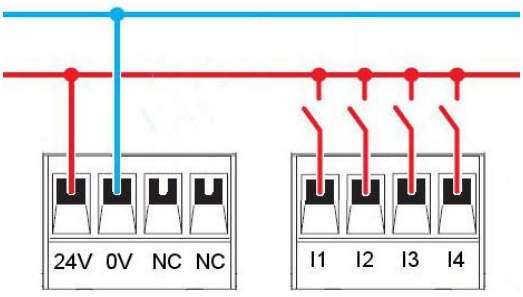


Bild Verdrahtung der Eingänge

Alarmierung per SMS

Oft ist eine einfache Emailbenachrichtigung nicht ausreichend wenn z.B. ein kritischer Grenzwert bei einer Anlage überschritten wird und das Servicepersonal per email gerade nicht erreichbar ist.
In diesem Fall kann man einfach einen Email zu SMS Dienst nutzen.
Über solch einen EMail to SMS Gateway kann man direkt EMails als SMS an ein Handy senden.
Evtl. anfallende Kosten für den SMS Versand bitte mit dem Provider abklären.

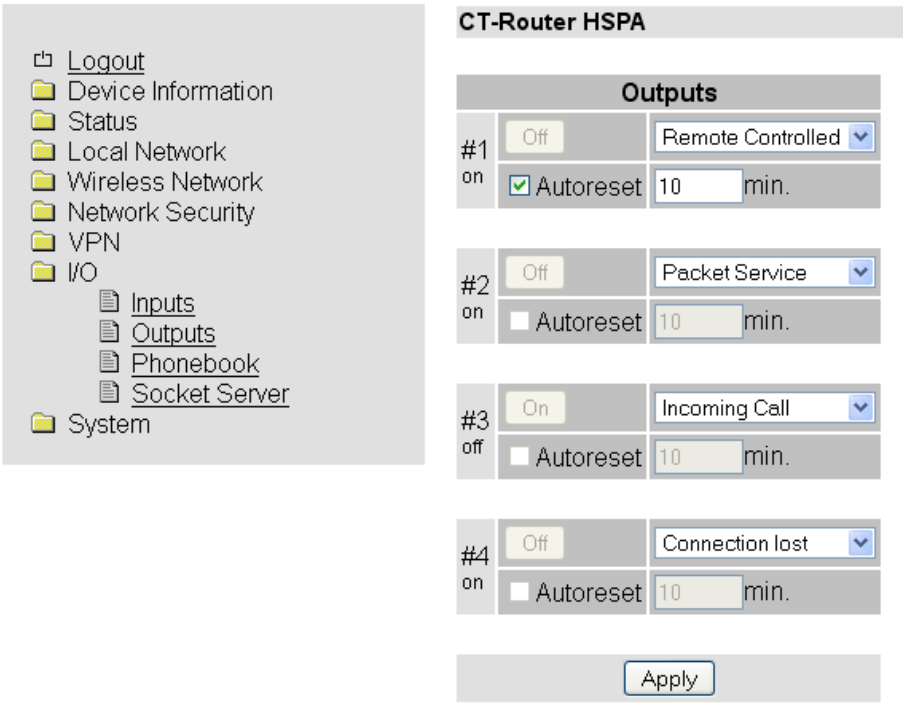
Einrichten eines Email zu SMS Gateway

Fast alle Provider bieten diesen Service mittlerweile an. Der Dienst muss lediglich mit einer einfachen SMS aktiviert werden.
Sie erhalten dann per SMS Ihre persönliche E-Mail-Adresse, die sich in der Regel aus der Rufnummer und dem Gateway-Namen zusammensetzt. Wenn Sie also T-Mobile Kunde sind und Ihre Handynummer die 0170/1234567 wäre, würde die Emailadresse „01701234567@ t-mobile-sms.de" lauten. Analog ist das für die anderen Netzte zu übernehmen.

Unten in der Tabelle finden Sie die Gateways und die Aktivierungsnummern der größten Anbieter.

Provider	email Adresse	Aktivierung Text	Aktivierung Nr.	Deaktivierung Text	Deaktivierung Nr.
TMobile	t-mobile-sms.de	OPEN	8000	CLOSE	8000
Vodafone	vodafone-sms.de	OPEN	3400	CLOSE	3400
EPlus	smsmail.eplus.de	START	7676245	STOP	7676245
O2 Germany	o2online.de	OPEN	6245	STOP	6245

Outputs



I/O →Outputs	
Outputs	Erklärung
Optionen	**Manual:** An- / Ausschalten erfolgt manuell über das WBM **Remote Controlled:** An- / Ausschalten per Steuerbefehl an den Socket Server (siehe Seite 44 und 55). Zusätzlich kann die Funktion Autoreset genutzt werden, bei der eine Zeitspanne in Minuten festgesetzt wird. **VPN Service:** Ausgang wird geschaltet, falls eine VPN-Verbindung besteht. **Connection Lost:** Der Ausgang wird geschaltet, wenn der Connection Check des Routers die konfigurierte Adresse nicht erreicht **Internet Link:** Ausgang wird geschaltet wenn eine Verbindung zum Internet aufgebaut ist.
Autoreset	Zeitraum in Minuten festlegen, nachdem der Ausgang zurückgesetzt wird.

Die kurzschlussfesten Schaltausgänge (O1 ... O4) sind für maximal 150 mA bei 10 ... 30 V DC ausgelegt.

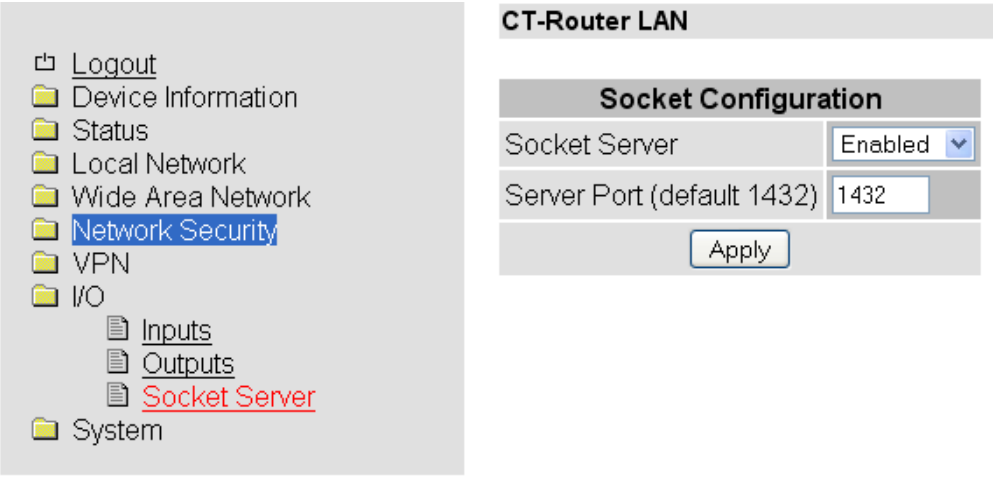
Das 0-V-Potential der Schaltausgänge müssen Sie an die "0 V" Klemme des Spg-Anschlusses anschließen

Socket Server

Der Router besitzt einen integrierten Socket Server und kann über den Empfang von XML-Dateien:

- I/O Signale setzen und abfragen
- Messages wie E-Mail und SMS versenden
- Den Router-Status abfragen

Für die Nutzung dieser Funktionen muss der Socket Server auf „Enable“ gesetzt werden. Der Port des Socket Servers
ist frei konfigurierbar, default ist Port = 1432



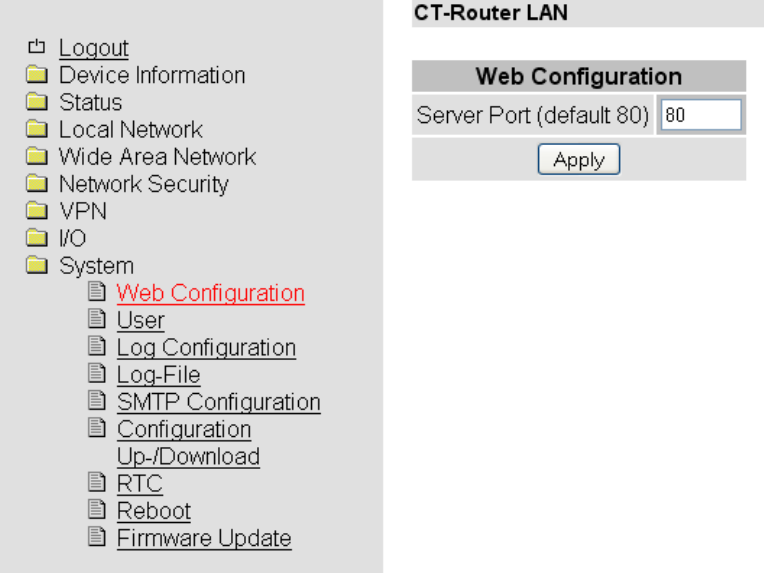
I/O → Socket Server	
Socket Server	Erklärung
Socket Server	**Disable:** Ansteuern des Routers über Ethernet deaktiviert **Enable:** Ansteuern des Routers über Ethernet aktiviert
Server Port (default 1432)	Socket Server Port festlegen (Port 80 kann nicht genutzt werden). Daten, die an den Router geschickt werden, müssen XML Version 1.0 konform sein. Beispiel: <?xml version="1.0"?> <io> <input no="1" value="on"> <output no="2" value="off"> <output no="3" /> </io>

Weiter Informationen siehe Punkt „Abfrage und Steuerung über XML Dateien“ auf Seite 55

System

Im Systemmenü können allgemeine Einstellungen für den CT-Router LAN getroffen werden.

Web Configuration

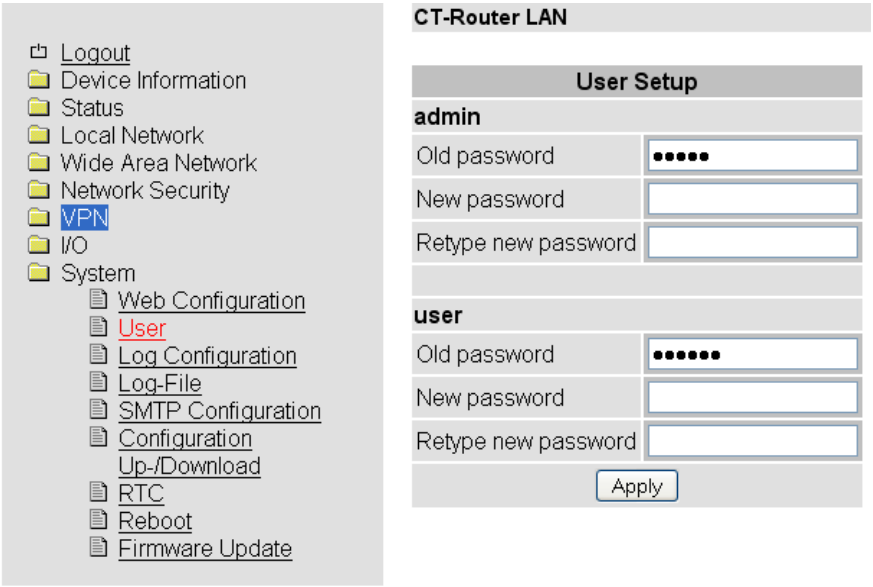


System → Web Configuration	
Web Configuration	**Erklärung**
Server Port (default 80)	Das Webinterface des Routers ist standardmäßig über den Port 80 zu erreichen. Der Server Port kann hier geändert werden. Geben Sie unter „Server Port“ den neuen Port ein und klicken Sie „Apply“.

Die Funktion wird erst nach einem Neustart des Routers wirksam. Starten Sie den Router neu – siehe Punkt „Reboot“. Merken Sie sich den neuen Port. Der neue Port muss jetzt beim Aufruf des Webinterfaces mit in dem Adressfeld des Browsers übergeben werden.

Beispiel: IP-Adresse des Routers: 192.168.0.1
Neuer Server Port des Routers: 81
Für die Konfiguration geben Sie jetzt http://192.168.0.1:81 in den Browser ein.

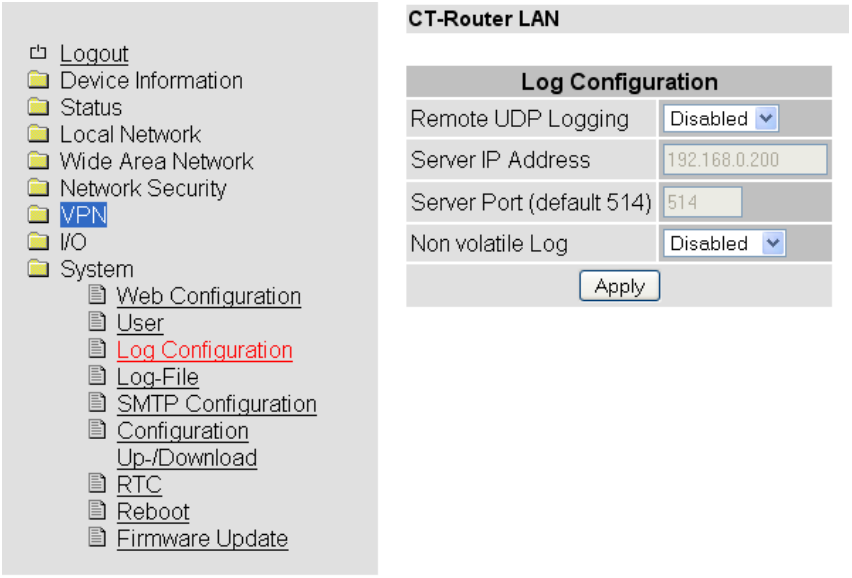
User



System → User	
User	Erklärung
admin	Uneingeschränkter Zugriff (Schreiben und Lesen) Neues Passwort festlegen
user	Eingeschränkter Zugriff (nur Lesen / nicht alle Bereiche) Neues Passwort festlegen

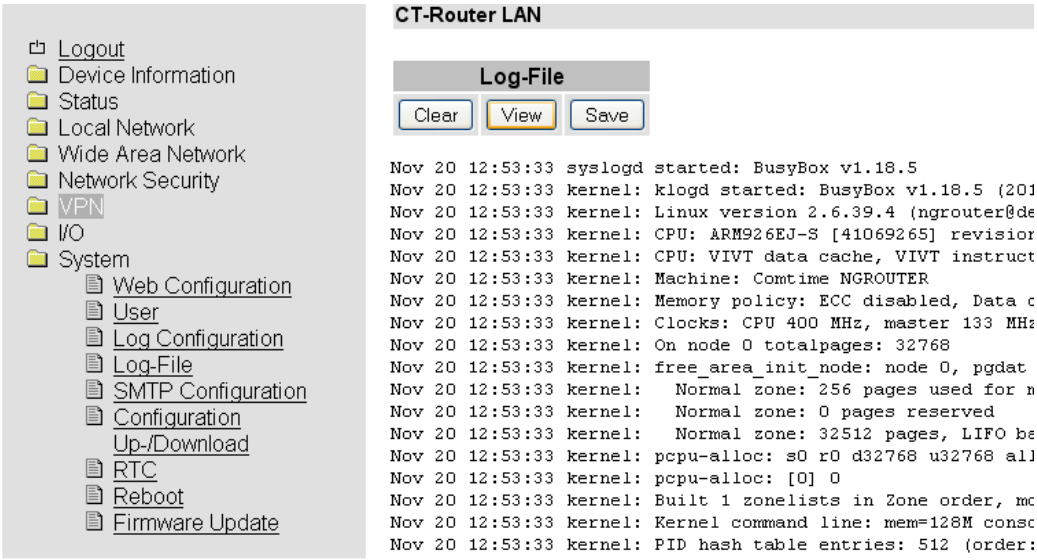
Log Configuration

Log-Files können via UDP auf einem externen Log-Server abgelegt werden.



System → Log Configuration	
Log Configuration	**Erklärung**
Remote UPD Logging	Log-Files können via UDP auf einem externen Log-Server abgelegt werden **Disabled:** Externes Logging deaktiviert **Enabled:** Externes Logging aktiviert
Server IP Address	IP-Adresse vom externen Log-Server
Server Port (default 514)	Port vom externen Log-Server
Non volatile Log	**Disable:** Speichert das Log intern auf einem vorher festgelegten Server. **USB-Stick:** Speichert das Log auf einem USB-Stick. Der USB-Stick muss am Router angeschlossen werden! **SD-Card:** Speichert das Log auf einer SD-Karte.

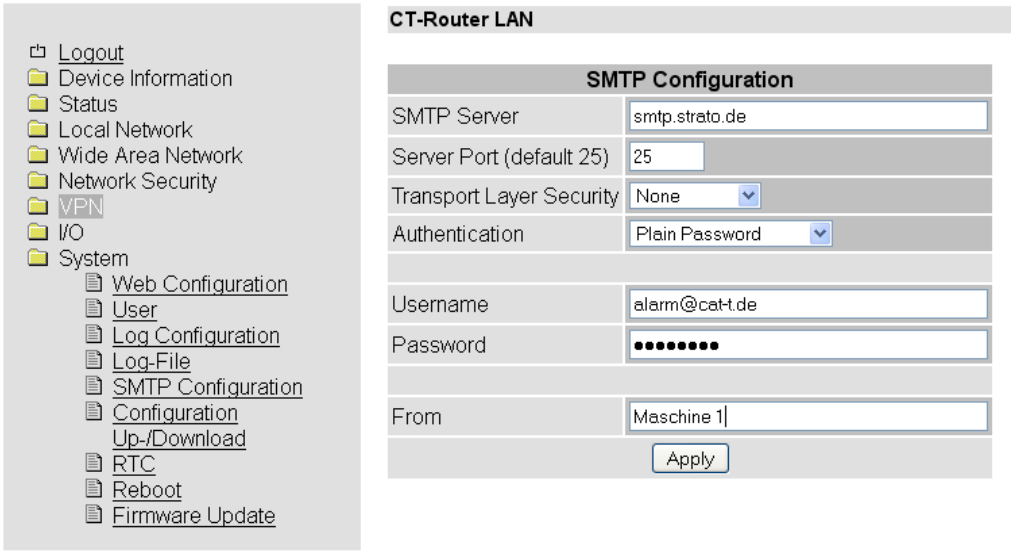
Log-File


Logout
Device Information
Status
Local Network
Wide Area Network
Network Security
VPN
I/O
System
Web Configuration
User
Log Configuration
Log-File
SMTP Configuration
Configuration Up-/Download
RTC
Reboot
Firmware Update
CT-Router LAN
Log-File
Clear
View
Save
Nov 20 12:53:33 syslogd started: BusyBox v1.18.5
Nov 20 12:53:33 kernel: klogd started: BusyBox v1.18.5 (201
Nov 20 12:53:33 kernel: Linux version 2.6.39.4 (ngrouter@de
Nov 20 12:53:33 kernel: CPU: ARM926EJ-S [41069265] revisior
Nov 20 12:53:33 kernel: CPU: VIVT data cache, VIVT instruct
Nov 20 12:53:33 kernel: Machine: Comtime NGROUTER
Nov 20 12:53:33 kernel: Memory policy: ECC disabled, Data c
Nov 20 12:53:33 kernel: Clocks: CPU 400 MHz, master 133 MHz
Nov 20 12:53:33 kernel: On node 0 totalpages: 32768
Nov 20 12:53:33 kernel: free_area_init_node: node 0, pgdat
Nov 20 12:53:33 kernel: Normal zone: 256 pages used for m
Nov 20 12:53:33 kernel: Normal zone: 0 pages reserved
Nov 20 12:53:33 kernel: Normal zone: 32512 pages, LIFO ba
Nov 20 12:53:33 kernel: pcpu-alloc: s0 r0 d32768 u32768 all
Nov 20 12:53:33 kernel: pcpu-alloc: [0] 0
Nov 20 12:53:33 kernel: Built 1 zonelists in Zone order, mo
Nov 20 12:53:33 kernel: Kernel command line: mem=128M consc
Nov 20 12:53:33 kernel: PID hash table entries: 512 (order:

System → Log-File	
Log-File	Erklärung
Clear	Einträge im internen Log-File werden gelöscht
View	Log-File Einträge werden im Browser-Fenster angezeigt
Save	Log-File wird gespeichert

SMTP Configuration

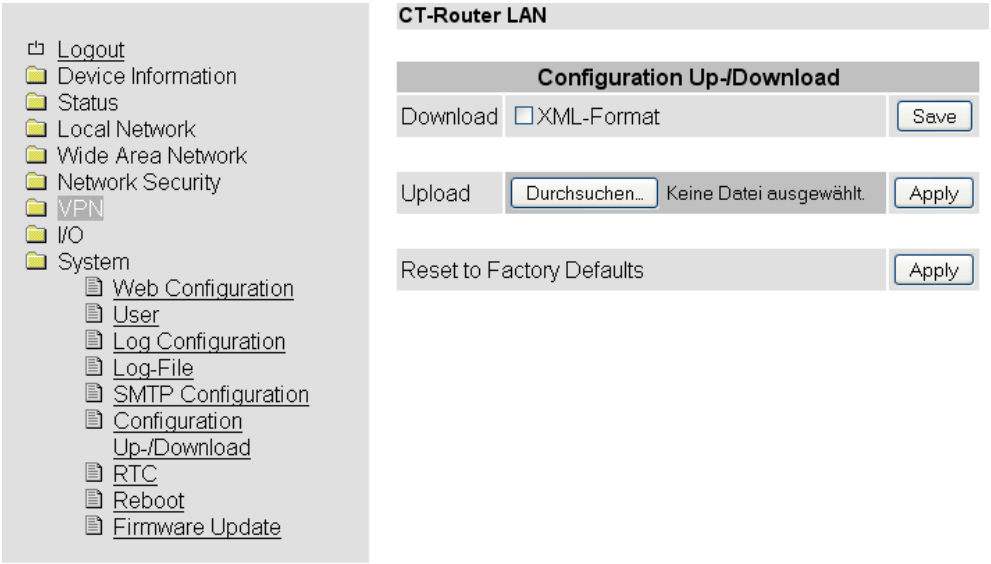
Für die Konfiguration verwenden Sie bitte die Zugangsdaten Ihres gewählten E-Mail Accounts



System →SMTP Configuration	
SMTP Configuration	Erklärung
SMTP Server	IP-Adresse / Hostname des SMTP Servers
SMTP Port (default 25)	Port des SMTP Servers
Transport Layer Security	Verschlüsselung: Keine, STARTTLS, SSL/TLS
Authentication	No authentication: Keine Authentifizierung notwendig Plain Password: Authentifizierung Benutzername und Passwort (unverschlüsselte Übertragung der Authentifizierungsdaten). Encrypted Password: Authentifizierung mit Benutzername und Passwort (verschlüsselte Übertragung der Authentifizierungsdaten)
Username	Benutzername
Password	Passwort
From	Absender der Mail

Configuration Up-/Download

Die Konfiguration kann als CFG-Datei (default) oder als XML-Datei auf dem Bediener-PC gespeichert werden. Auf diesem PC gespeicherte Konfigurationen können in den Router geladen werden.



System → Configuration Up-/Download	
Up-/Download	**Erklärung**
Download	Aktuelle Konfigurationen herunterladen
Upload	Gesicherte oder veränderte Konfigurationen hochladen und mit "apply" bestätigen.
Reset to Factory Defaults	Konfigurationen und IP-Einstellungen auf Werkeinstellung zurücksetzen. Hochgeladene Zertifikate bleiben erhalten.

Konfiguration über SSH und XML-Datei

Die Übertragung einer XML-Datei zur Konfiguration des Routers kann zusätzlich mittels des SSH Protokolls über die lokale Ethernet-Schnittstelle oder im Remote Betrieb erfolgen.

SSH bzw. Secure Shell bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe
man eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellen kann.
Verwenden Sie unter **Linux** die Konsoleneingabe. Unter **Windows** empfehlen wir Ihnen die Verwendung der unter
putty.org downloadbaren Programme **plink.exe** und **pscp.exe**.

Die Beispiele unten basieren auf den Default-Einstellungen des Routers:

Benutzername:	admin
Passwort:	admin
Router IP-Adresse:	192.168.0.1

Download der Konfiguration per SSH

Sie können die Konfiguration des Routers als XML-Datei oder als TGZ-Datei herunterladen.

Unter Linux:
ssh admin@192.168.0.1 'su -c "/usr/sbin/export_cfg"' > config.xml
oder
ssh admin@192.168.0.1 'su -c "/usr/sbin/export_cfg tgz"' > config.tgz

Unter Windows mit PLINK.EXE
plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/export_cfg\"" > config.xml
oder
plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/export_cfg tgz\"" > config.tgz

Upload der Konfiguration per SSH

Unter Linux:
Ohne Router-Reboot:

cat config.xml | ssh admin@192.168.0.1 'su -c "/usr/sbin/store_cfg"'

Mit anschließendem Router-Reboot:

cat config.xml | ssh admin@192.168.0.1 'su -c "/usr/sbin/store_cfg; /sbin/reboot"'

Das Passwort wird hier von SSH interaktiv erfragt. Ein automatischer Batch Betrieb ist damit nicht möglich. Allerdings ist es mit dem Programm "sshpass" möglich eine Script-Datei samt Passwort ausführen zu lassen.

Die Script-Datei z.B. cfgupl.sh muss folgendes enthalten:
#!/bin/bash cat config.xml | ssh admin@192.168.0.1 'su -c "/usr/sbin/store_cfg; /sbin/reboot"'
Der Linux-Befehl lautet dann: *sshpass -padmin ./cfgupl.sh*

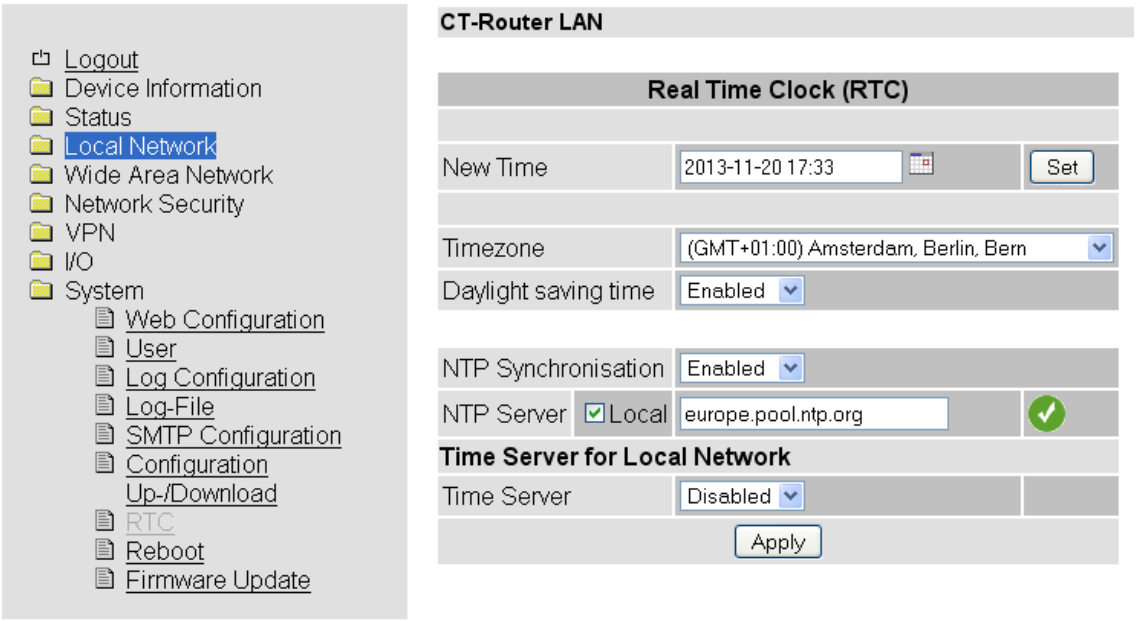
Unter Windows mit PSCP.EXE und PLINK.EXE
Ohne Router-Reboot:

pscp -scp -pw admin config.xml admin@192.168.0.1:/tmp/cfg.xml
plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/store_cfg /tmp/cfg.xml\""

Mit anschließendem Router-Reboot:

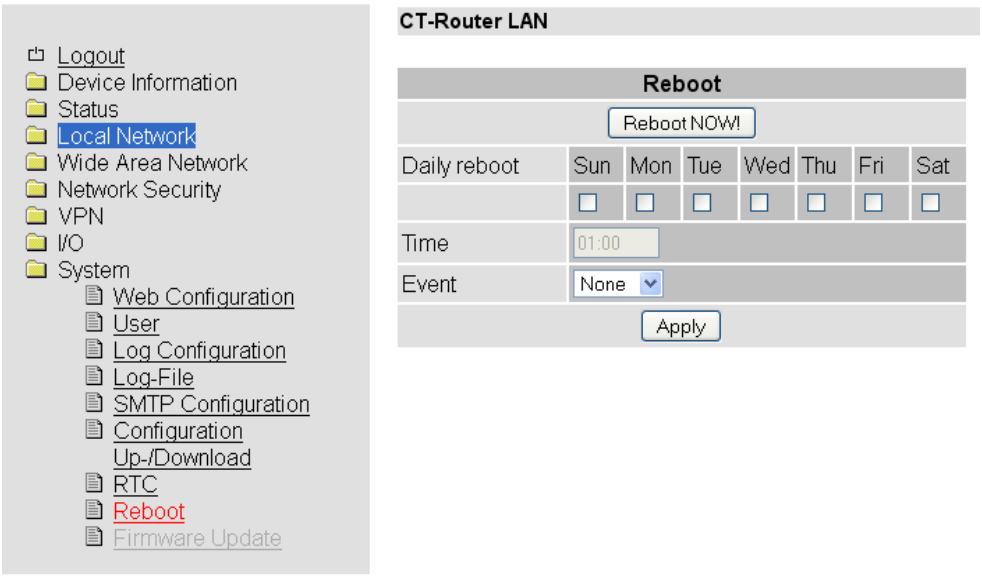
pscp -scp -pw admin config.xml admin@192.168.0.1:/tmp/cfg.xml
plink -2 -pw admin admin@192.168.0.1 "su -c \"/usr/sbin/store_cfg /tmp/cfg.xml; /sbin/reboot\""

RTC



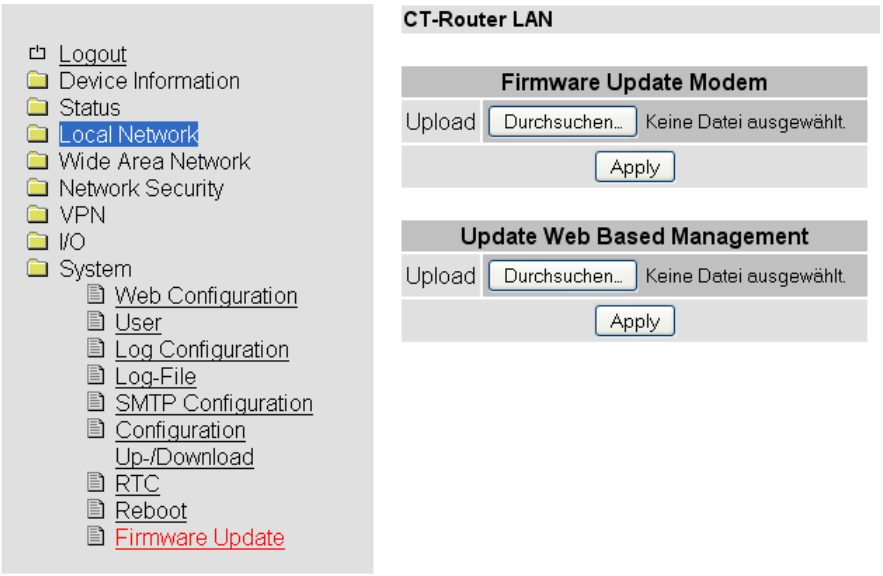
System → RTC	
RTC	**Erklärung**
New Time	Manuelle Zeitkonfiguration, falls kein NTP-Server vorhanden ist.
Timezone	Zeitzonenauswahl
Daylight saving time	**Disable:** Sommerzeitberücksichtigung deaktiviert **Enable:** Sommerzeitberücksichtigung aktiviert
NTP Synchronisation	Datum und Uhrzeit können mit einem NTP-Server synchronisiert werden. Bei Erstverwendung dieser Funktion kann die erste Synchronisation bis zu 15 Minuten dauern.
NTP Server	Im LAN-Netzwerk kann der Router als NTP-Server eingestellt werden. Es wird hierzu eine Adresse von enem NTP-Server benötigt. Die NTP Synchronisation muss auf Enable gestellt werden.
Time Server	**Disable:** Zeitserverfunktion für das lokale Netzwerk deaktiviert **Enable:** Zeitserverfunktion für das lokale Netzwerk aktiviert

Reboot



System → Reboot	
Reboot	**Erklärung**
Reboot NOW!	Sofortigen Neustart des Routers erzwingen!
Daily reboot	Den Router an bestimmten Wochentagen zum bestimmten Zeitpunkt neustarten. Mit Klicken auf die Kontrollkästchen legen Sie die Wochentage für den Neustart fest.
Time	Uhrzeit des Neustarts (Stunde:Minute)
Event	Router kann mit digitalem Eingang neugestartet werden. Signal sollte nach einem Neustart wieder "Low" sein.

Firmware Update



System → Firmware Update	
Reboot	Erklärung
Firmware Update Modem	Diese Updates sorgen für Funktionserweiterungen und Produktaktualisierungen.
Update Web Based Management	Diese Updates beziehen sich auf die Konfiguration über einen Internetbrowser.

Format der XML Dateien

Jede Datei beginnt mit dem Header:
<?xml version="1.0"?>
oder
<?xml version="1.0" encoding="UTF-8"?>

Gefolgt von dem Basis-Eintrag. Folgende Basis-Einträge stehen zur Auswahl:
<io> </io> # E/A-System
<info> </info> # Allgemeine Informationen abfragen
<cmgr ...> </cmgr> # SMS versenden (nur Mobilfunkgeräte)
<email ...> </email> # eMail versenden

Alle Daten werden in UTF-8 kodiert. Folgende Zeichen müssen
als Sequenzen übertragen werden:
& - &
< - <
> - >
" - "
' - '

Beispiele zu den Basis-Einträgen:

a) E/A System

```
<?xml version="1.0"?>
<io>
<output no="1"/>                    # Zustand von Ausgang 1 abfragen
<output no="2" value="on"/>         # Ausgang 2 einschalten
<input no="1"/>                     # Zustand von Eingang 1 abfragen
</io>
```

Hinweis: Als "value" kann sowohl on/off als auch 0/1 angegeben werden.
Zurückgegeben wird immer on oder off.

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<io>
<output no="1" value="off"/> # Zustand von Ausgang 1; hier eingeschaltet
<output no="2" value="on"/> # Zustand von Ausgang 2; wurde eingeschaltet
<input no="1" value="off"/> # Zustand von Eingang 1; hier ausgeschaltet
</io>
</result>
```

Zu beachten ist, das Ausgänge, welche ferngesteuert werden sollen, als"Remote Controlled" konfiguriert sein müssen.

b) Allgemeine Informationen abfragen

```
<?xml version="1.0"?>
<info>
<device /> # Gerätedaten abfragen
<radio /> # Daten zur Funkverbindung abfragen (nur Mobilfunkgeräte)
</info>
```

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<info>
<device>
<serialno>13120004</serialno>
<hardware>A</hardware>
<firmware>1.00.4-beta</firmware>
<wbm>1.34.8</wbm>
<imei>359628040604790</imei>
</device>
<radio>
<provider>Vodafone.de</provider>
<rssi>15</rssi>
<creg>1</creg>
<lac>0579</lac>
<ci>26330CD</ci>
<packet>0</packet>
</radio>
</info>
</result>
```

c) SMS versenden (nur Mobilfunkgeräte)

```
<?xml version="1.0"?>
<cmgs destaddr="0123456789">Dies ist der SMS-Text</cmgs>
Zurückgeliefert wird etwa folgendes:
<?xml version="1.0" encoding="UTF-8"?>
<result>
<cmgs length="98">SMS accepted</cmgs>
</result>
```

d) eMail versenden

```
<?xml version="1.0"?>
<email to="x.yz@diesunddas.de" cc="info@andere.de">
<subject>Test Mail</subject>
<body>
    Dies ist ein mehrzeiliger eMail-Text.
    mfg.
    ihr Router
</body>
</email>
```

Zurückgeliefert wird etwa folgendes:

<?xml version="1.0" encoding="UTF-8"?>
<result>
<email>done</email>
</result>
oder im Fehlerfall:
<?xml version="1.0" encoding="UTF-8"?>
<result>
<email error="3">transmisson failed</email>
</result>

Hinweis zur Darstellung: die Einrückungen und Zeilenumbrüche dienen nur der Verständlichkeit und müssen so nicht gesendet werden, noch werden sie so gesendet. Alle empfangenen Daten sollten mit einem XML-Parser wie z.B. Expat interpretiert werden.

Daten senden und empfangen

Der Kommunikationsablauf ist folgender:

- Verbindung zum Socket-Server aufbauen
- Daten senden
- Zurückgegebene Daten mit XML-Parser interpretieren

Verbindung schließen

Funktions-Test mittels Windows Hyperterminal

Für einen Test kann unter Windows das bekannte Programm „Hyperterminal" verwendet werden. Über Hyperterminal können XML-Dateien an den Socket Server des Routers gesendet werden. Die entsprechenden XML-Dateien (siehe Kapitel „Abfrage und Steuerung über XML Dateien") müssen dafür vorab auf Ihren Bediener-PC gespeichert worden sein.
Öffnen Sie Hyperterminal und konfigurieren Sie die gewünschte Verbindung (Hier ein Beispiel unter der Verwendung von Default-Einstellungen):

Hostadresse: 192.168.0.1 (IP-Adresse des Routers / Socket Servers)
Anschlussnummer: 1432 (Port des Socket Servers)
Verbindung herstellen über: TCP/IP (Winsock)

Öffnen Sie die Verbindung und wählen Sie im Menü von Hyperterminal „Übertragung / Textdatei senden...." die zu übertragende XML-Datei aus.

Nach der erfolgreichen Übertragung erhalten Sie die Antwort auf Ihre Anfrage.

Applikationsbeispiel